IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MONTANA
BUTTE DIVISION

IN RE: SNOWFLAKE, INC. DATA SECURITY BREACH LITIGATION	**Case No. 2:24-MD-03126-BMM**

PLAINTIFFS' REPRESENTATIVE CLASS ACTION COMPLAINT

TABLE OF CONTENTS

INTRODUCTION

1. Data companies are acutely aware of the critical importance of cybersecurity in an increasingly interconnected world. With the exponential growth of cloud storage, companies are entrusted with sensitive information, ranging from personal details to financial records.

2. This is a "hub-and-spoke" data breach case. The "hub" in this case is Defendant Snowflake, which is a company that specializes in cloud-storage technologies to warehouse and secure sensitive data, and in selling data storage and analytics products. Snowflake sells its data storage services to numerous companies, or "spokes," who store information on Snowflake's data cloud. These spokes included Defendants[1] Ticketmaster, Advance Auto Parts, LendingTree, and AT&T.

[1] The Defendants in this consolidated MDL are Snowflake, Inc. ("Snowflake"); Ticketmaster, LLC and Live Nation Entertainment, Inc. (referred to collectively as "Ticketmaster" or the "Ticketmaster Defendants"); Advance Auto Parts, Inc. and Advance Stores Company, Inc. (referred to collectively as "Advance Auto" or the "Advance Auto Defendants"); LendingTree, LLC, and Quotewizard.com, LLC (referred to collectively as "LendingTree" or the "LendingTree Defendants"); and AT&T, Inc. and AT&T Mobility, LLC (referred to collectively as "AT&T" or the "AT&T Defendants"). The non-Snowflake Defendants are referred to herein collectively as the "Spoke Defendants."

3. Stressing to investors that it built its data-storage product "with security as a core tenet,"[2] Snowflake has long understood and acknowledged the importance of robust cybersecurity to protect consumer data.

4. Similarly, the Spoke Defendants have also long understood the importance of robust cybersecurity, as discussed herein, to protect the data of their own customers, employees, and subscribers—information from which Defendants, themselves, extract a handsome profit. The Spoke Defendants include Fortune 500 corporations and have a collective market capitalization totaling hundreds of billions of dollars.

5. Information security policies and practices are imperative to ensure that sensitive information is not exposed to unauthorized third parties. These exposures, commonly referred to as "data breaches," can cause significant harm to individuals—exposing them to fraud and attempted fraud, identity theft, reputational harm, and the continuing risk of harm that results from criminals having their sensitive information.

6. A single data breach can result in catastrophic consequences for individuals. As a result, and based upon legal and industry-standard requirements, companies prioritize robust cybersecurity measures.

---

[2] Snowflake Inc. 2024 Annual Report (Form 10-K) at 15 (Mar. 26, 2024) ("Snowflake 2024 10-K"), https://d18rn0p25nwr6d.cloudfront.net/CIK-0001640147/264ea0e0-8e73-4f07-9f54-78ab341a2c79.pdf.

7. In this case, however, none of the Defendants implemented three of the most basic and industry-standard cybersecurity policies to protect Personal Information, including most prominently, multifactor authentication (MFA).[3] The foreseeable result: a massive data breach (the "Data Breach"). The cybercriminal group known by codename UNC5537 used compromised login credentials for Defendants, plugged them in to Spoke Defendants' Snowflake accounts, and successfully exfiltrated Personal Information belonging to hundreds of millions of consumers.

8. UNC5537's success was made possible by basic data security failings on the part of Snowflake and the Spoke Defendants. These companies collectively flouted relevant governmental guidance, regulations, statutes, and industry standards.

[3] "Personal Information," as used herein, refers to that information which was exposed to cybercriminals through the Data Breach. While the information exposed varies from each Spoke Defendant, each protected that information behind credentials (i.e., a username and password), intending that it would not be exposed to unauthorized third parties. As alleged herein, inadequate, negligent, and reckless cybersecurity practices resulted in that information being exposed.

9. The Data Breach's foreseeable consequences are neither imaginary nor hypothetical: shortly after the Data Breach, sensitive information previously stored with Snowflake began appearing for sale on the dark web.[4]

10. Plaintiffs and Class Members[5] now face the real and actual harm that the Data Breach has caused them and will continue to cause them. Not only have cybercriminals obtained valuable and sensitive Personal Information about them, but that information has been obtained by other criminals and offered for resale to still more criminals. As a result, Plaintiffs and Class Members have already experienced fraud or attempted fraud, an invasion of their privacy, time and expenses spent mitigating the imminent and substantial risk of data misuse, and are at significant risk of identity theft, reputational harm, and other injuries.

11. Each Defendant bears responsibility for its role in the Data Breach. Despite their experience and sophistication, Defendants were negligent (at best) and reckless (at worst) for failing to implement basic and routinely required cybersecurity practices to protect Plaintiffs' and Class Members' Personal Information.

---

[4] Snowflake Breach Threat Actor Offers Data of Cloud Company's Customers, SOCRadar, https://socradar.io/overview-of-the-snowflake-breach/ (last accessed Jan. 13, 2025).

[5] "Class Members" refers to those individuals who were impacted by the Data Breach, as alleged herein. Specific class definitions for each Defendant are provided in the relevant sections.

PARTIES

I. Defendants

12. **Snowflake Inc.** is a cloud-based data storage company incorporated under Delaware law, with its principal place of business located at 106 E. Babcock Street, Suite 3A, Bozeman, Montana.[6]

13. **AT&T, Inc.** is a telecommunications company incorporated under Delaware law, with its principal place of business located at 208 S. Akard Street, Dallas, Texas.[7] Cricket Wireless is a wholly owned subsidiary of AT&T.[8] AT&T has agreements with Mobile Virtual Network Operators ("MVNOs") such as Boost Mobile and Consumer Cellular under which the MVNOs pay to use AT&T's network infrastructure.

14. **AT&T Mobility, LLC** is a telecommunications company, which is a wholly owned subsidiary of AT&T, Inc.[9] AT&T Mobility, LLC is a Delaware

---

6 Snowflake Inc. 2024 10-K at 1.

7 AT&T Inc. Annual Report (Form 10-K) (Feb. 23, 2024) ("AT&T 2023 10-K"), https://investors.att.com/~/media/Files/A/ATT-IR-V2/financial-reports/annual-reports/2023/2023-complete-annual-report.pdf.

8 Chris Welch, *FCC approves AT&T's purchase of Leap Wireless, says 'it's in the public interest,'* The Verge (Mar. 13, 2014), https://www.theverge.com/2014/3/13/5505798/fcc-approves-att-purchase-of-leap-wireless. Cricket Wireless nevertheless has a separate brand identity, including separate marketing, logo, brand assets, as well as an independent retail presence from AT&T. The average consumer does not know of any relationship between Cricket and AT&T.

9 AT&T 2023 10-K at 1.

limited liability company, with its principal place of business located at 1025 Lenox Park Blvd. NE, Atlanta, Georgia.[10]

15. **Live Nation Entertainment, Inc.** is an entertainment company incorporated under Delaware law, with its principal place of business located at 9348 Civic Center Drive, Beverly Hills, California.[11]

16. **Ticketmaster, LLC** is a ticket distribution company for entertainment events, and is a wholly owned subsidiary of Live Nation.[12] Ticketmaster is a Virginia limited liability company, with its principal place of business located at 9348 Civic Center Drive, Beverly Hills, California.[13]

17. **Advance Auto Parts, Inc.** is a provider of automotive aftermarket parts incorporated under Delaware law, with its principal place of business located at 4200 Six Forks Road, Raleigh, North Carolina.[14]

---

[10] AT&T Mobility, LLC, *Annual Registration*, Ga. Corps. Div., https://ecorp.sos.ga.gov/BusinessSearch/DownloadFile?filingNo=26582594.

[11] Live Nation Entertainment, Inc., Annual Report (Form 10-K) (Feb. 22, 2024) ("Live Nation 2023 10-K"), https://www.sec.gov/Archives/edgar/data/1335258/000133525824000017/lyv-20231231.htm.

[12] Live Nation 2023 10-K at 54.

[13] Ticketmaster, LLC, *Statement of Information*, Cal. Sec'y of State (Sept. 25, 2024), https://bizfileonline.sos.ca.gov/api/report/GetImageByNum/253133124121113249074045085047228112143236158047.

[14] Advance Auto Parts, Inc. Annual Report *amendment* (Form 10-K/A) (May 29, 2024) ("Advance Auto 2023 10-K"), https://www.sec.gov/ix?doc=/Archives/edgar/data/1158449/000115844924000128/aap-20231230.htm.

18. **Advance Stores Company, Inc.** is a wholly owned subsidiary of Advance Auto Parts.[15] Advance Stores Company is incorporated under Virginia law, with its principal place of business located at 4200 Six Forks Road, Raleigh, North Carolina.[16]

19. **LendingTree, LLC** is an online lending company incorporated under Delaware law, with its principal place of business located at 1415 Vantage Park Drive, Suite 700, Charlotte, North Carolina.[17] LendingTree, Inc. is the parent of LT Intermediate Company, LLC, which holds all the outstanding ownership interests of LendingTree, LLC.[18]

20. **QuoteWizard.com, LLC** is an insurance comparison company, and a wholly owned subsidiary of LendingTree.[19] QuoteWizard is a Delaware limited

---

15 *Id.* at 15.

16 Advance Stores Company, Inc. 2023 Annual Report, N.C. Sec'y of State (Jan. 8, 2024), https://www.sosnc.gov/online_services/business_registration/flow_annual_report/4978817.

17 LendingTree, LLC 2023 Annual Report, N.C. Sec'y of State (Mar. 20, 2024), https://www.sosnc.gov/online_services/business_registration/flow_annual_report/7314197.

18 LendingTree 2023 10-K at 7.

19 LendingTree, Inc. Form 8-K/A Exhibit 2.1 (Oct. 12, 2018), https://www.sec.gov/ix?doc=/Archives/edgar/data/0001434621/000143462124000006/tree-20231231.htm.

liability company, with its principal place of business located at 1415 Vantage Park Drive, Suite 700, Charlotte, North Carolina.[20]

II. Plaintiffs

21. Each of the Plaintiffs below brings causes of action against Defendant Snowflake as well as an individual Spoke Defendant, as outlined herein.

A. Ticketmaster Plaintiffs

22. **Plaintiff Eric Anderson** is a citizen of New York residing in Jamestown. Plaintiff Anderson received a data breach notice letter, via U.S. mail, directly from Ticketmaster, in around July 2024. Plaintiff Anderson is a customer of Ticketmaster, since at least 2011. Plaintiff Anderson has maintained an account on Ticketmaster's website to purchase event tickets, and in doing so, provided Ticketmaster with at least his name, address, email, phone number, and payment card information.

23. After the Data Breach began, in May 2024, Plaintiff Anderson experienced fraudulent activity on both of his debit cards. His primary card had five unauthorized charges, prompting the bank to close the card and issue a replacement. Additionally, his secondary card had one fraudulent charge, which he had to dispute before also arranging for its closure and reissuance.

---

[20] QuoteWizard.com, LLC 2023 Annual Report, N.C. Sec'y of State (Jan. 8, 2024), https://www.sosnc.gov/online_services/business_registration/flow_annual_report/15286870.

24. In May 2024, Plaintiff Anderson was informed by his credit card company that his personal information was found on the dark web. Since the Data Breach, Plaintiff Anderson has experienced an increase in spam calls and spam texts. Since the Data Breach, Plaintiff Anderson has spent approximately 10-15 hours investigating and mitigating against the substantial risks presented by the theft of his Personal Information. These mitigation efforts have included, but are not limited to, addressing fraudulent activity on his debit cards and actively monitoring his credit accounts and reports.

25. As a result of the Data Breach, Plaintiff Anderson has suffered injury and damages, including but not limited to, the unauthorized use of his stolen Personal Information; the substantial risk of identity theft and reasonable mitigation efforts spent to protect against such risks, including time and expenses spent obtaining credit monitoring services and reviewing financial accounts for fraudulent activity; loss of property and value of that property with respect to the inability to control use of his Personal Information; invasion of his privacy; and emotional distress and anxiety resulting from the theft of his Personal Information and responding to identity theft.

26. Plaintiff Anderson is very careful about sharing his own Personal Information and has never knowingly transmitted unencrypted Personal Information over the internet or any other unsecured source. Plaintiff Anderson is

diligent about keeping hard copy documents containing Personal Information secure, and is diligent about the online security of his accounts.

27. **Plaintiff Charles Fitzgerald** is a citizen of New York residing in Buffalo. Plaintiff Fitzgerald is a current customer of Ticketmaster, last purchased a ticket in or around Fall of 2022, and, in doing so, provided Ticketmaster with at least his name, address, email, phone number, and payment card information. Plaintiff Fitzgerald became aware of the Ticketmaster Data Breach in late May or early June 2024 via social media.

28. After the Data Breach began, in early fall of 2024, Plaintiff Fitzgerald received a notice that an unknown party had attempted to make unauthorized charges on the debit card linked with his Ticketmaster account. He spent time and resources responding to the fraud alert and taking appropriate preventative measures, including having the card reissued.

29. After the Data Breach, Plaintiff Fitzgerald was informed via a credit monitoring service that his personal information was found on the dark web, including, at a minimum, his name, address, phone number, and email address. Since the Data Breach, Plaintiff Fitzgerald has spent approximately 5 hours investigating and mitigating against the substantial risks presented by the theft of his Personal Information. These mitigation efforts have included monitoring transactions, changing passwords, and reviewing and investigating dark web alerts.

30. As a result of the Data Breach, Plaintiff Fitzgerald has suffered injury and damages, including but not limited to, the unauthorized use of his stolen Personal Information; the substantial risk of identity theft and reasonable mitigation efforts spent to protect against such risks, including time spent reviewing financial accounts for fraudulent activity; loss of property and value of that property with respect to the inability to control use of his Personal Information; invasion of his privacy; and emotional distress and anxiety resulting from the theft of his Personal Information and responding to identity theft.

31. Plaintiff Fitzgerald is very careful about sharing his own Personal Information and has never knowingly transmitted unencrypted Personal Information over the internet or any other unsecured source. Plaintiff Fitzgerald is diligent about keeping hard copy documents containing Personal Information secure, and is diligent about the online security of his accounts.

32. **Plaintiff Susie Garcia** is a citizen of California residing in Riverside. Plaintiff Garcia has been a customer of Ticketmaster for over 10 years and last purchased a ticket in April 2023, when she provided Ticketmaster with her name, address, email, phone number, and credit card information. She does not remember logging into her Ticketmaster account after this date.

33. In December 2024, Plaintiff Garcia suffered multiple fraudulent charges on her Wells Fargo debit card equaling $80. Plaintiff Garcia disputed the charges and had to replace her debit card.

34. In the time following the Data Breach, Plaintiff Garcia was informed by Experian that her information was found on the dark web.

35. Since the Data Breach, Plaintiff Garcia has spent approximately 2-3 hours investigating and mitigating against the substantial risks presented by the theft of her Personal Information. These mitigation efforts have included freezing her credit with credit agencies, monitoring her credit accounts and reports, changing her passwords, and researching the breach.

36. As a result of the Data Breach, Plaintiff Garcia has suffered injury and damages, including but not limited to, the unauthorized use of her stolen Personal Information; the substantial risk of identity theft and reasonable mitigation efforts spent to protect against such risks, including time and expenses spent reviewing financial accounts for fraudulent activity; loss of property and value of that property with respect to the inability to control use of her Personal Information; invasion of her privacy; and emotional distress and anxiety resulting from the theft of her Personal Information and addressing the identity theft.

37. Plaintiff Garcia is very careful about sharing her own Personal Information and has never knowingly transmitted unencrypted Personal

Information over the internet or any other unsecured source. Plaintiff Garcia is diligent about keeping hard copy documents containing Personal Information secure, and is diligent about the online security of her accounts.

38. **Plaintiff Valerie Lozoya** is a citizen of California residing in Hawthorne. Plaintiff Lozoya received a data breach notice letter, via U.S. mail, directly from Ticketmaster, dated July 17, 2024. Plaintiff Lozoya is a current customer of Ticketmaster and has regularly purchased tickets. In doing so, she provided Ticketmaster with at least her name, address, email, phone number, and payment card information.

39. After the Data Breach began, this past November 2024, Plaintiff Lozoya received a notice from her credit union that an unauthorized party had attempted to make charges on her debit card. Her credit union required her to shut her card down and receive a new one.

40. Since the Data Breach, Plaintiff Lozoya has experienced an increase in spam and receives approximately 3-4 spam calls and 1-2 spam texts a day. Since the Data Breach, Plaintiff Lozoya has spent approximately 5-6 hours investigating and mitigating against the substantial risks presented by the theft of her Personal Information. She continues to monitor her accounts for any fraudulent activity. Her mitigation efforts have included contacting her credit union, closing her debit card

and receiving a new card, setting up new auto billing accounts, and monitoring her credit accounts and reports.

41. As a result of the Data Breach, Plaintiff Lozoya has suffered injury and damages, including but not limited to, the unauthorized use of her stolen Personal Information; the substantial risk of identity theft and reasonable mitigation efforts spent to protect against such risks, including time and expenses spent obtaining credit monitoring services and reviewing financial accounts for fraudulent activity; loss of property and value of that property with respect to the inability to control use of her Personal Information; invasion of her privacy; and emotional distress and anxiety resulting from the theft of her Personal Information and responding to identity theft.

42. Plaintiff Lozoya is very careful about sharing her own Personal Information and has never knowingly transmitted unencrypted Personal Information over the internet or any other unsecured source. Plaintiff Lozoya is diligent about keeping hard copy documents containing Personal Information secure, and is diligent about the online security of her accounts.

43. **Plaintiff LaVonne Madden** is a citizen of Montana residing in Shepherd. Plaintiff Madden received a data breach notice letter, via U.S. mail, directly from Ticketmaster in July 2024. Plaintiff Madden is a former customer of Ticketmaster, and believes she last purchased a ticket in 2008 and in doing so,

provided Ticketmaster with at least her name, address, email, phone number, and payment card information.

44. After receiving the data breach notice letter, Plaintiff Madden spent at least four hours of time and resources responding to the fraud and freezing her credit with Equifax and TransUnion and contacting her bank.

45. As a result of the Data Breach, Plaintiff Madden has suffered injury and damages, including but not limited to, the unauthorized use of her stolen Personal Information; the substantial risk of identity theft and reasonable mitigation efforts spent to protect against such risks, including time spent obtaining credit freezes and reviewing financial accounts for fraudulent activity; loss of property and value of property with respect to the inability to control use of her Personal Information; invasion of her privacy; and emotional distress and anxiety resulting from the theft of her Personal Information and responding to identity theft.

46. Plaintiff Madden is very careful about sharing her own Personal Information and has never knowingly transmitted unencrypted Personal Information over the internet or any other unsecured source. Plaintiff Madden is diligent about keeping hard copy documents containing Personal Information secure, and is diligent about the online security of her accounts.

47. **Plaintiff Jolinda Murphy** is a citizen of Montana residing in Missoula. Plaintiff Murphy received a data breach notice letter, via U.S. mail,

directly from Ticketmaster, dated July 17, 2024. Plaintiff Murphy is a customer of Ticketmaster, but she cannot recall the last time she purchased tickets. She does recall that, when she did purchase tickets, she provided Ticketmaster with at least her name, address, email, phone number, and payment card information.

48. After the data breach in May 2024, Plaintiff Murphy experienced an increase in spam and receives approximately 3-4 spam calls and 1-2 spam texts a day, along with several spam emails. Many of the texts include fraudulent links claiming she and her husband owe fines or are missing packages and request them to click a link. Since the Data Breach, Plaintiff Murphy has spent increased time weekly and monthly reviewing account information as well as constantly blocking and deleting the spam texts and emails she and her husband receive.

49. As a result of the Data Breach, Plaintiff Murphy has suffered injury and damages, including but not limited to, the substantial risk of identity theft and reasonable mitigation efforts spent to protect against such risks, including time and expenses spent obtaining credit monitoring services and reviewing financial accounts for fraudulent activity; loss of property and value of that property with respect to the inability to control use of her Personal Information; invasion of her privacy; and emotional distress and anxiety resulting from the theft of her Personal Information.

50. Plaintiff Murphy is very careful about sharing her own Personal Information and has never knowingly transmitted unencrypted Personal Information over the internet or any other unsecured source. Plaintiff Murphy is diligent about keeping hard copy documents containing Personal Information secure, and is diligent about the online security of her accounts.

51. **Plaintiff Lauren Neve** is a citizen of California residing in San Juan Capistrano. Plaintiff Neve is a former customer of Ticketmaster, where she last purchased a ticket in 2022 and in doing so, provided Ticketmaster with at least her name, address, email, and payment card information.

52. After the Data Breach occurred, Plaintiff Neve was informed by her credit card company that her personal information was found on the dark web. Since the Data Breach, Plaintiff Neve has experienced an increase in spam and receives approximately 3-4 spam calls and 1-2 spam texts a day. Since the Data Breach, Plaintiff Neve has spent approximately 6-7 hours investigating and mitigating against the substantial risks presented by the theft of her Personal Information. These mitigation efforts have included freezing her credit with credit agencies, registering for credit monitoring services, and monitoring her credit accounts and reports.

53. As a result of the Data Breach, Plaintiff Neve has suffered injury and damages, including but not limited to, the unauthorized use of her stolen Personal

Information; the substantial risk of identity theft and reasonable mitigation efforts spent to protect against such risks, including time and expenses spent obtaining credit monitoring services and reviewing financial accounts for fraudulent activity; loss of property and value of that property with respect to the inability to control use of her Personal Information; invasion of her privacy; and emotional distress and anxiety resulting from the theft of her Personal Information and responding to identity theft.

54. Plaintiff Neve is very careful about sharing her own Personal Information and has never knowingly transmitted unencrypted Personal Information over the internet or any other unsecured source. Plaintiff Neve is diligent about keeping hard copy documents containing Personal Information secure, and is diligent about the online security of her accounts.

55. **Plaintiff Molly O'Hara** is a citizen of Massachusetts residing in Revere. Plaintiff O'Hara received a data breach notice letter, via U.S. mail, directly from Ticketmaster, dated July 9, 2024. Plaintiff O'Hara is a current customer of Ticketmaster who has regularly purchased tickets. In doing so, she provided Ticketmaster with at least her name, address, email, phone number, and payment card information.

56. In 2024, Plaintiff O'Hara was informed by her bank through a credit monitoring program that her personal information was found on the dark web. Since

the Data Breach, Plaintiff O'Hara has experienced an increase in spam emails, texts and calls and receives approximately 3-4 spam calls and 3-4 spam texts a day. Since the Data Breach, Plaintiff O'Hara has spent approximately 6-7 hours investigating and mitigating against the substantial risks presented by the theft of her Personal Information. These mitigation efforts have included registering for credit monitoring services, resetting passwords, resetting auto billing payments and monitoring her credit accounts and reports.

57. As a result of the Data Breach, Plaintiff O'Hara has suffered injury and damages, including but not limited to, the unauthorized use of her stolen Personal Information; the substantial risk of identity theft and reasonable mitigation efforts spent to protect against such risks, including time and expenses spent obtaining credit monitoring services and reviewing financial accounts for fraudulent activity; loss of property and value of that property with respect to the inability to control use of her Personal Information; invasion of her privacy; and emotional distress and anxiety resulting from the theft of her Personal Information and responding to identity theft.

58. Plaintiff O'Hara is very careful about sharing her own Personal Information and has never knowingly transmitted unencrypted Personal Information over the internet or any other unsecured source. Plaintiff O'Hara is

diligent about keeping hard copy documents containing Personal Information secure, and is diligent about the online security of her accounts.

59. **Plaintiff Dekima Thomas** is a citizen and resident of the District of Columbia. Plaintiff D. Thomas received a data breach notice letter, via U.S. mail, directly from Ticketmaster in or around July 2024. Plaintiff D. Thomas is a customer of Ticketmaster.

60. Since at least 2013, Plaintiff D. Thomas has maintained an account on Ticketmaster's website to purchase event tickets, and in doing so, provided Ticketmaster with at least her name, address, email, phone number, and payment card information.

61. In or around the fall of 2024, Plaintiff D. Thomas was notified by Credit Karma that her personal information had been discovered on the dark web. Since the Data Breach, she has experienced a significant increase in spam, receiving an additional 4-5 spam messages per day since April.

62. Since the Data Breach, Plaintiff D. Thomas has dedicated approximately 8 to 10 hours to investigating and mitigating the significant risks resulting from the theft of her Personal Information. Her mitigation efforts include, but are not limited to, enrolling in credit monitoring services and actively monitoring her credit accounts and reports.

63. As a result of the Data Breach, Plaintiff D. Thomas has suffered injury and damages, including but not limited to, the unauthorized use of her stolen Personal Information; the substantial risk of identity theft and reasonable mitigation efforts spent to protect against such risks, including time and expenses spent obtaining credit monitoring services and reviewing financial accounts for fraudulent activity; loss of property and value of that property with respect to the inability to control use of her Personal Information; invasion of her privacy; and emotional distress and anxiety resulting from the theft of her Personal Information and responding to identity theft.

64. Plaintiff D. Thomas is very careful about sharing her own Personal Information and has never knowingly transmitted unencrypted Personal Information over the internet or any other unsecured source. Plaintiff D. Thomas is diligent about keeping hard copy documents containing Personal Information secure, and is diligent about the online security of her accounts.

65. **Plaintiff Christina Xian** is a citizen of California residing in Millbrae. Plaintiff Xian is a former customer of Ticketmaster, where she last purchased a ticket in 2024 and in doing so, provided Ticketmaster with at least her name, address, email, phone number, and PayPal account information for payment.

66. After the Data Breach began, in May 2024, Plaintiff Xian received a notice that an unauthorized party had gained access to her Ticketmaster account

spending $2,554.66 in resale tickets using her PayPal account, which was attached to her Ticketmaster account for payment purposes. Plaintiff Xian was forced to spend time and resources responding to the fraud and changing her passwords with PayPal and Ticketmaster.

67. Since the Data Breach, Plaintiff Xian has spent approximately 3 hours investigating and mitigating against the substantial risks presented by the theft of her Personal Information. These mitigation efforts have included changing passwords to accounts, removing automated payments from her PayPal account, and signing up for a password monitoring service.

68. As a result of the Data Breach, Plaintiff Xian has suffered injury and damages, including but not limited to, the unauthorized use of her stolen Personal Information; the substantial risk of identity theft and reasonable mitigation efforts spent to protect against such risks, including time and expenses spent obtaining a password monitoring service and reviewing financial accounts for fraudulent activity; loss of property and value of that property with respect to the inability to control use of her Personal Information; and invasion of her privacy from the theft of her Personal Information and responding to identity theft.

69. Plaintiff Xian is very careful about sharing her own Personal Information and has never knowingly transmitted unencrypted Personal Information over the internet or any other unsecured source. Plaintiff Xian is

diligent about keeping hard copy documents containing Personal Information secure, and is diligent about the online security of her accounts.

B. Advance Auto Plaintiffs

70. **Plaintiff Emmanuel Chaidez** is a citizen of Illinois residing in Normal. Plaintiff Chaidez received a data breach notice letter, via U.S. mail, directly from Advance Auto, dated July 10, 2024. Plaintiff Chaidez previously applied for and accepted an offer of employment with Advance Auto. In the course of this employment process, Plaintiff Chaidez provided Advance Auto with his Personal Information, including, at least, his Social Security number, full name, address, date of birth, phone number, email address, and work history.

71. Since the Data Breach, Plaintiff Chaidez has experienced an increase in spam and receives approximately 25 spam calls per day. Since the Data Breach, Plaintiff Chaidez has spent approximately 40 hours investigating and mitigating against the substantial risks presented by the theft of his Personal Information. These mitigation efforts have included closely monitoring his financial accounts, resetting automatic billing instructions tied to compromised accounts, driving to his bank branch to address incidences of identity theft, and time spent on the phone with his bank and credit card companies.

72. As a result of the Data Breach, Plaintiff Chaidez has suffered injury and damages, including but not limited to, the unauthorized use of his stolen

Personal Information; the substantial risk of identity theft and reasonable mitigation efforts spent to protect against such risks, including time and expenses spent obtaining credit monitoring services and reviewing financial accounts for fraudulent activity; loss of property and value of that property with respect to the inability to control use of his Personal Information; invasion of his privacy; and emotional distress and anxiety resulting from the theft of his Personal Information and responding to identity theft.

73. Plaintiff Chaidez is very careful about sharing his own Personal Information and has never knowingly transmitted unencrypted Personal Information over the internet or any other unsecured source. Plaintiff Chaidez is diligent about keeping hard copy documents containing Personal Information secure, and is diligent about the online security of his accounts.

74. **Plaintiff Stefondra Monroe** is a citizen of Florida residing in Clewiston. Plaintiff Monroe received a data breach notice letter, via U.S. mail, directly from Advance Auto dated July 10, 2024. Plaintiff Monroe submitted an application for employment with Advance Auto several years ago, which required that she provide Advance Auto with her personal details including her full name, address, email address, date of birth, employment information/work history, and Social Security number. Plaintiff Monroe never ultimately accepted an offer of employment with Advance Auto.

75. Since the Data Breach, Plaintiff Monroe has spent approximately 3-4 hours investigating the Data Breach and mitigating against the substantial risks presented by the theft of her Personal Information. These mitigation efforts have included monitoring her financial accounts and reviewing notices to investigate unauthorized charges.

76. As a result of the Data Breach, Plaintiff Monroe has suffered injury and damages, including but not limited to, the unauthorized use of her stolen Personal Information; the substantial risk of identity theft and reasonable mitigation efforts spent to protect against such risks, including time and expenses spent reviewing financial accounts for fraudulent activity; loss of property and value of that property with respect to the inability to control use of her Personal Information; invasion of her privacy; and emotional distress, anxiety, and annoyance resulting from the theft of her Personal Information and responding to identity theft.

77. Plaintiff Monroe is very careful about sharing her own Personal Information and has never knowingly transmitted unencrypted Personal Information over the internet or any other unsecured source. Plaintiff Monroe is diligent about keeping hard copy documents containing Personal Information secure, and is diligent about the online security of her accounts.

78. **Plaintiff Raymond Moule** is a citizen of Connecticut residing in Enfield. Plaintiff Moule received a data breach notice letter, via U.S. mail, directly

from Advance Auto, dated July 10, 2024. Plaintiff Moule applied for and accepted employment with Advance Auto in 2017. In the course of this employment process, Plaintiff Moule provided Advance Auto with his Personal Information, including, at least, his Social Security number, driver's license, full name, address, date of birth, phone number, email address, and work history.

79. After the Data Breach, Plaintiff Moule has received notice that multiple individuals have attempted to fraudulently open credit cards in his name. Plaintiff Moule has spent significant time and resources responding to the fraud, and this fraud has caused significant financial and emotional strain.

80. Since the Data Breach, Plaintiff Moule has experienced an increase in spam calls, emails, and text messages. Since the Data Breach, Plaintiff Moule has spent many hours investigating and mitigating against the substantial risks presented by the theft of his Personal Information. These mitigation efforts have included closely monitoring his financial accounts, changing his passwords, calling banks regarding the alerts of fraudulent attempts to open credit cards in his name, and signing up for credit monitoring services.

81. As a result of the Data Breach, Plaintiff Moule has suffered injury and damages, including but not limited to, the unauthorized use of his stolen Personal Information; the substantial risk of identity theft and reasonable mitigation efforts spent to protect against such risks, including time and expenses spent obtaining

credit monitoring services and reviewing financial accounts for fraudulent activity; loss of property and value of that property with respect to the inability to control use of his Personal Information; invasion of his privacy; and emotional distress and anxiety resulting from the theft of his Personal Information and responding to identity theft.

82. Plaintiff Moule is very careful about sharing his own Personal Information and has never knowingly transmitted unencrypted Personal Information over the internet or any other unsecured source. Plaintiff Moule is diligent about keeping hard copy documents containing Personal Information secure, and is diligent about the online security of his accounts.

83. **Plaintiff Raven Richardson** is a citizen of Mississippi residing in South Haven. Plaintiff Richardson received a data breach notice letter, via U.S. mail, directly from Advance Auto dated July 10, 2024. Plaintiff Richardson submitted an application for employment with Advance Auto in or about 2023, which required that she provide Advance Auto with her personal details including her full name, address, email address, phone number, date of birth, employment information/work history, and Social Security number. Plaintiff Richardson never ultimately accepted an offer of employment with Advance Auto.

84. Since the Data Breach, Plaintiff Richardson has spent approximately 1 hour investigating the Data Breach and mitigating against the substantial risks

presented by the theft of her Personal Information. These mitigation efforts have included changing passwords on several of her online accounts.

85. As a result of the Data Breach, Plaintiff Richardson has suffered injury and damages, including but not limited to, the unauthorized use of her stolen Personal Information; the substantial risk of identity theft and reasonable mitigation efforts spent to protect against such risks, including time and expenses spent reviewing financial accounts for fraudulent activity; loss of property and value of that property with respect to the inability to control use of her Personal Information; invasion of her privacy; and emotional distress, anxiety, and annoyance resulting from the theft of her Personal Information and responding to identity theft.

86. Plaintiff Richardson is very careful about sharing her own Personal Information and has never knowingly transmitted unencrypted Personal Information over the internet or any other unsecured source. Plaintiff Richardson is diligent about keeping hard copy documents containing Personal Information secure, and is diligent about the online security of her accounts.

87. **Plaintiff Don Smith** is a citizen of Illinois residing in Hanover Park. Plaintiff Smith received a data breach notice letter, via U.S. mail, directly from Advance Auto, dated July 10, 2024. Plaintiff Smith applied for and accepted an offer of employment with Advance Auto. In the course of this employment process, Plaintiff Smith provided Advance Auto with his Personal Information, including, at

least, his Social Security number, full name, address, date of birth, phone number, email address, and work history.

88. Since the Data Breach, Plaintiff Smith has experienced an increase in spam and phishing calls, emails, and text messages. Since the Data Breach, Plaintiff Smith has spent numerous hours investigating and mitigating against the substantial risks presented by the theft of his Personal Information. These mitigation efforts have included closely monitoring his financial accounts, changing his account passwords, reviewing transaction histories and credit statements, and researching online the best practices for protecting himself from identity theft and fraud.

89. As a result of the Data Breach, Plaintiff Smith has suffered injury and damages, including but not limited to, the unauthorized use of his stolen Personal Information; the substantial risk of identity theft and reasonable mitigation efforts spent to protect against such risks, including time and expenses spent reviewing financial accounts for fraudulent activity; loss of property and value of that property with respect to the inability to control use of his Personal Information; invasion of his privacy; and emotional distress and anxiety resulting from the theft of his Personal Information and responding to identity theft.

90. Plaintiff Smith is very careful about sharing his own Personal Information and has never knowingly transmitted unencrypted Personal Information over the internet or any other unsecured source. Plaintiff Smith is

diligent about keeping hard copy documents containing Personal Information secure, and is diligent about the online security of his accounts.

91. **Plaintiff Raymond Swain** is a citizen of California residing in Bakersfield. Plaintiff Swain received a data breach notice letter, via U.S. mail, directly from Advance Auto, dated July 10, 2024. Plaintiff Swain applied for employment with Advance Auto. In the course of this application process, Plaintiff Swain provided Advance Auto with his Personal Information, including, among other things, his Social Security number, full name, address, date of birth, phone number, email address, and work history

92. Since the Data Breach, Plaintiff Swain has experienced an increase in spam calls and text messages. Since the Data Breach, Plaintiff Swain has spent significant time investigating and mitigating against the substantial risks presented by the theft of his Personal Information. These mitigation efforts have included time spent verifying the legitimacy of the Data Breach notice letter and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred.

93. As a result of the Data Breach, Plaintiff Swain has suffered injury and damages, including but not limited to, the unauthorized use of his stolen Personal Information; the substantial risk of identity theft and reasonable mitigation efforts spent to protect against such risks, including time and expenses spent obtaining credit monitoring services and reviewing financial accounts for fraudulent activity;

loss of property and value of that property with respect to the inability to control use of his Personal Information; invasion of his privacy; and emotional distress and anxiety resulting from the theft of his Personal Information and responding to identity theft.

94. Plaintiff Swain is very careful about sharing his own Personal Information and has never knowingly transmitted unencrypted Personal Information over the internet or any other unsecured source. Plaintiff Swain is diligent about keeping hard copy documents containing Personal Information secure, and is diligent about the online security of his accounts.

C. LendingTree Plaintiffs

95. **Plaintiff Aaron Macom** is a citizen of Washington State residing in Allyn. Plaintiff Macom received a data breach notice letter, via U.S. mail, directly from QuoteWizard, dated July 30, 2024. Plaintiff Macom is a former customer of LendingTree, where he sought to obtain loan services, provided LendingTree with at least his name, address, phone number, email address, financial information, date of birth, employment information, and Social Security number.

96. Plaintiff Macom has experienced an increase in spam and receives constant spam and phishing communications by phone calls and texts. Since the Data Breach, Plaintiff Macom has spent numerous hours investigating the Data Breach and mitigating against the substantial risks presented by the theft of his

Personal Information. These mitigation efforts have included vigilantly monitoring his credit accounts and reports and calling his credit card company.

97. As a result of the Data Breach, Plaintiff Macom has suffered injury and damages, including but not limited to, the unauthorized use of his stolen Personal Information; the substantial risk of identity theft and reasonable mitigation efforts spent to protect against such risks, including time and expenses spent obtaining credit monitoring services and reviewing financial accounts for fraudulent activity; loss of property and value of that property with respect to the inability to control use of his Personal Information; invasion of his privacy; and emotional distress, anxiety, and annoyance resulting from the theft of his Personal Information and responding to identity theft.

98. Plaintiff Macom is very careful about sharing his own Personal Information and has never knowingly transmitted unencrypted Personal Information over the internet or any other unsecured source. Plaintiff Macom is diligent about keeping hard copy documents containing Personal Information secure, and is diligent about the online security of his accounts.

99. **Plaintiff Antoun Nader** is a citizen of Washington residing in Everett. Plaintiff Nader received a data breach notice letter, via U.S. mail, directly from LendingTree in July 2024. Plaintiff Nader has submitted his information to LendingTree for purposes of obtaining insurance quotes, and as such provided

LendingTree with at least his name, address, phone number, email, gender, marital status, income status and date of birth.

100. After receiving the data breach notice letter, Plaintiff Nader spent at least four hours of time and resources responding to the fraud including checking his credit reports, watching his accounts, notifying his banks, notifying his credit card providers, calling Social Security, and calling various customer service support centers.

101. As a result of the Data Breach, Plaintiff Nader has suffered injury and damages, including but not limited to, the unauthorized use of his stolen Personal Information; the substantial risk of identity theft and reasonable mitigation efforts spent to protect against such risks, including time spent reviewing financial accounts for fraudulent activity and contacting banks and credit card issuers; loss of property and value of that property with respect to the inability to control use of his Personal Information; invasion of his privacy; and emotional distress and anxiety resulting from the theft of his Personal Information and responding to identity theft.

102. Plaintiff Nader is very careful about sharing his own Personal Information and has never knowingly transmitted unencrypted Personal Information over the internet or any other unsecured source. Plaintiff Nader is

diligent about keeping hard copy documents containing Personal Information secure, and is diligent about the online security of his accounts.

103. **Plaintiff Linda Pierce** is a citizen of Texas residing in Jacksonville. Plaintiff Pierce received a data breach notice letter, via U.S. mail, directly from QuoteWizard, dated July 30, 2024. Plaintiff Pierce recalls applying for a loan through a LendingTree web-based application in the past 1-2 years and in so doing, provided LendingTree with at least her name, home address, email address, phone number, date of birth, driver's license number, Social Security number, and financial information.

104. Since the Data Breach, Plaintiff Pierce has received multiple emails from a credit monitoring service that her Personal Information was found on the dark web. Since the Data Breach, Plaintiff Pierce has experienced an increase in spam and receives numerous spam calls and multiple spam texts a day. Since the Data Breach, Plaintiff Pierce has spent approximately 30 hours investigating and mitigating against the substantial risks presented by the theft of her Personal Information. These mitigation efforts have included freezing her credit with Experian, registering for credit monitoring services, monitoring her credit accounts and reports, and changing her passwords regularly.

105. As a result of the Data Breach, Plaintiff Pierce has suffered injury and damages, including but not limited to, the unauthorized use of her stolen Personal

Information; the substantial risk of identity theft and reasonable mitigation efforts spent to protect against such risks, including time and expenses spent obtaining credit monitoring services and reviewing financial accounts for fraudulent activity; loss of property and value of that property with respect to the inability to control use of her Personal Information; invasion of her privacy; and emotional distress and worry resulting from the theft of her Personal Information and responding to identity theft.

106. Plaintiff Pierce is very careful about sharing her own Personal Information and has never knowingly transmitted unencrypted Personal Information over the internet or any other unsecured source. Plaintiff Pierce is diligent about keeping hard copy documents containing Personal Information secure, and is diligent about the online security of her accounts.

107. **Plaintiff Nathan Thomas** is a citizen of Washington residing in Bellingham, Washington. Plaintiff N. Thomas is a frequent user of LendingTree and received a notice letter from QuoteWizard dated July 30, 2024. In order to utilize services from LendingTree, Plaintiff N. Thomas provided LendingTree with his name, address, email address, phone number, and date of birth.

108. After the Data Breach, in June 2024, Plaintiff N. Thomas suffered multiple fraudulent charges totaling approximately $400. Near the end of 2024,

Plaintiff N. Thomas noticed that an unauthorized bank account was opened in his name.

109. As a result of the Data Breach, Plaintiff N. Thomas has suffered injury and damages, including but not limited to, the substantial risk of identity theft and reasonable mitigation efforts spent to protect against such risks, including time and expenses spent reviewing financial accounts for fraudulent activity; loss of property and value of that property with respect to the inability to control use of his Personal Information; invasion of his privacy; and emotional distress and anxiety resulting from the theft of his Personal Information and responding to identity theft.

110. Plaintiff N. Thomas is very careful about sharing his own Personal Information and has never knowingly transmitted unencrypted Personal Information over the internet or any other unsecured source. Plaintiff N. Thomas is diligent about keeping hard copy documents containing Personal Information secure, and is diligent about the online security of his accounts.

D. AT&T Plaintiffs

111. **Plaintiff Latosha Austin** is a citizen of California residing in Fresno. Plaintiff Austin is a current AT&T customer and has been a customer since 2000. Plaintiff Austin was also a customer of Cricket Wireless in or around 1999-2000. Plaintiff Austin received correspondence from AT&T in or around June 2024.

112. In October of 2024, Plaintiff Austin received a phone call from a number she recognized, which used to belong to her father, who recently had his number changed after receiving an onslaught of spam and phishing calls. The caller left a voicemail asking for money. Her father had not placed the call, nor left the voicemail.

113. In April, September, and November of 2024, Plaintiff Austin was informed that her information was found on the dark web. Since the Data Breach, Plaintiff Austin has experienced an increase in spam and receives approximately 1-2 spam texts a day.

114. Since the Data Breach, Plaintiff Austin has spent numerous hours investigating and mitigating against the substantial risks presented by the theft of her Personal Information. Without much guidance from AT&T, Plaintiff Austin performed reasonable security mitigation efforts, including freezing her credit with credit agencies, researching the breach, and monitoring her credit accounts and reports.

115. As a result of the Data Breach, Plaintiff Austin has suffered injury and damages, including but not limited to, the unauthorized use of her stolen Personal Information; the substantial risk of identity theft and reasonable mitigation efforts spent to protect against such risks, including reviewing financial accounts for fraudulent activity; loss of property and value of that property with respect to the

inability to control use of her Personal Information; invasion of her privacy; and emotional distress and anxiety resulting from the theft of her Personal Information and responding to identity theft.

116. Plaintiff Austin is very careful about sharing her own Personal Information and has never knowingly transmitted unencrypted Personal Information over the internet or any other unsecured source. Plaintiff Austin is diligent about keeping hard copy documents containing Personal Information secure, and is diligent about the online security of her accounts.

117. **Plaintiff Gilbert Criswell** is a citizen of California residing in San Francisco. Plaintiff Criswell is a current customer of AT&T and has been using its services for approximately 10 years.

118. In or around September 2024, Plaintiff Criswell received a notification from Google Security that his account information and password were compromised by AT&T, prompting him to change his password.

119. In December 2024, Plaintiff Criswell received a phone call from a trusted number. However, Plaintiff Criswell was notified by AT&T's security application Active Armor that the call originated from Russia. Therefore, Plaintiff did not engage with the caller and marked the call as spam. Around the same time, Active Armor also notified him that he was affected by a malicious malware attack,

prompting him to reset his mobile phone and backup the data contained in his phone.

120. In or around December 2024, Plaintiff Criswell was informed by Google Security that his information was found on the dark web. Since the Data Breach, Plaintiff Criswell has experienced an increase in spam and receives approximately 50 phishing emails and spam text messages a day. Since the Data Breach, Plaintiff Criswell spends approximately 4-5 hours a week investigating and mitigating against the substantial risks presented by the theft of his Personal Information. Without guidance from AT&T, Plaintiff Criswell engaged in reasonable mitigation efforts, including blocking spam calls, monitoring for phishing attempts, changing passwords, freezing his credit with credit agencies, researching the breach, and monitoring his credit accounts and reports.

121. As a result of the Data Breach, Plaintiff Criswell has suffered injury and damages, including but not limited to, the unauthorized use of his stolen Personal Information; the substantial risk of identity theft and reasonable mitigation efforts spent to protect against such risks, including time and expenses spent obtaining credit monitoring services and reviewing financial accounts for fraudulent activity; loss of property and value of that property with respect to the inability to control use of his Personal Information; invasion of his privacy; and

emotional distress and anxiety resulting from the theft of his Personal Information and responding to identity theft.

122. Plaintiff Criswell is very careful about sharing his own Personal Information and has never knowingly transmitted unencrypted Personal Information over the internet or any other unsecured source. Plaintiff Criswell is diligent about keeping hard copy documents containing Personal Information secure, and is diligent about the online security of his accounts.

123. Plaintiff **Roscoe Eldridge** is a citizen of Illinois residing in South Beloit. Plaintiff Eldridge is not a customer of AT&T, Cricket Wireless, or AT&T's MVNOs. He does frequently communicate with individuals who use those phone carriers, however, and did so throughout 2022. For example, his daughter has had a Cricket Wireless account for over a decade, and he was in frequent contact with her through phone calls and texts throughout 2022.

124. After the Data Breach began, in May 2024, Plaintiff Eldridge was informed by his Discover card account and Experian account that his personal information was found on the dark web. Since the Data Breach, Plaintiff Eldridge has continued to receive approximately two dark web notifications per week. Since the Data Breach, Plaintiff Eldridge has experienced an increase in spam and receives approximately 15 spam calls a day and 2-3 spam texts a week. Since the Data Breach, Plaintiff Eldridge has spent approximately 40 hours investigating and

mitigating against the substantial risks presented by the theft of his Personal Information. These mitigation efforts have included freezing his credit with credit agencies and monitoring his credit accounts and reports.

125. As a result of the Data Breach, Plaintiff Eldridge has suffered injury and damages, including but not limited to, the unauthorized use of his stolen Personal Information; the substantial risk of identity theft and reasonable mitigation efforts spent to protect against such risks, including time and expenses spent obtaining credit freezes and reviewing financial accounts for fraudulent activity; loss of property with respect to the inability to control use of his Personal Information; invasion of his privacy; and emotional distress and anxiety resulting from the theft of his Personal Information and responding to identity theft. Since the Data Breach, in September 2024, Plaintiff Eldridge developed a bleeding ulcer, which he believes was a result of the anxiety related to the Data Breach and its consequences.

126. Plaintiff Eldridge is very careful about sharing his own Personal Information and has never knowingly transmitted unencrypted Personal Information over the internet or any other unsecured source. Plaintiff Eldridge is diligent about keeping hard copy documents containing Personal Information secure, and is diligent about the online security of his accounts.

127. **Plaintiff David Hornthal** is a citizen of Illinois residing in Deerfield. Plaintiff Hornthal is and during all times concerned herein was a user on his father's AT&T account. In connection with receiving phone services from AT&T, his father provided AT&T with at least Plaintiff Hornthal's payment card information.

128. After the Data Breach began, AT&T sent a data breach notice via email dated July 15, 2024, to the main contact for Plaintiff Hornthal's AT&T account, his father. The notice email listed Plaintiff Hornthal's phone number among those whose data was accessed in the Data Breach.

129. On or about November 17, 2024, an unauthorized party made a fraudulent charge on the credit card Plaintiff Hornthal used to pay for AT&T's services. Plaintiff Hornthal spent time and resources responding to the fraud, including investigating the fraudulent charge, contacting his bank, and closing and reopening the affected account. Plaintiff Hornthal also spent approximately 2-3 hours resetting automatic billing instructions tied to the affected credit card and addressing fees incurred from failed automatic billing attempts on the closed card.

130. Since the Data Breach, Plaintiff Hornthal has experienced a significant increase in the number of spam calls and texts he receives. Plaintiff Hornthal has spent approximately 1-2 hours of additional time investigating and mitigating against the substantial risks presented by the theft of his Personal Information. Without guidance from AT&T, Plaintiff Hornthal engaged in reasonable mitigation

efforts, including researching the details of the Data Breach and monitoring his financial accounts and credit score.

131. As a result of the Data Breach, Plaintiff Hornthal has suffered injury and damages, including but not limited to, the unauthorized use of his stolen Personal Information; actual fraud in the form of unauthorized charges on his credit card; the substantial risk of identity theft and reasonable mitigation efforts spent to protect against such risks, including time and expenses spent reviewing financial accounts and his credit report for fraudulent activity; loss of property and value of that property with respect to the inability to control use of his Personal Information; invasion of his privacy; and emotional distress and anxiety resulting from the theft of his Personal Information and responding to identity theft.

132. Plaintiff Hornthal is very careful about sharing his own Personal Information and has never knowingly transmitted unencrypted Personal Information over the internet or any other unsecured source. Plaintiff Hornthal is diligent about keeping hard copy documents containing Personal Information secure, and is diligent about the online security of his accounts.

133. **Plaintiff Traci Lively** is a citizen and resident of the District of Columbia. Plaintiff Lively has been a Cricket Wireless customer since approximately 2022. Cricket's customers, like Plaintiff Lively, suffered from the Data Breach in part as a result of Cricket Wireless's use of AT&T's network.

134. Plaintiff Lively received a notice letter from Cricket Wireless dated July 16, 2024. In the fall of 2024, Plaintiff Lively was informed that there had been approximately ten inquiries into his credit, relating to opening unauthorized accounts and loans.

135. Since the Data Breach, Plaintiff Lively has spent countless hours investigating and mitigating against the substantial risks presented by the theft of his Personal Information. Without guidance from AT&T or Cricket, Plaintiff Lively performed reasonable mitigation efforts, including monitoring his credit accounts and reports, researching the breach, and addressing attempts of unauthorized use of his Personal Information.

136. As a result of the Data Breach, Plaintiff Lively has suffered injury and damages, including but not limited to, the unauthorized use of his stolen Personal Information; the substantial risk of identity theft and reasonable mitigation efforts spent to protect against such risks, including time and expenses spent reviewing financial accounts for fraudulent activity; loss of property and value of that property with respect to the inability to control use of his Personal Information; invasion of his privacy; and emotional distress and anxiety resulting from the theft of his Personal Information and responding to identity theft.

137. Plaintiff Lively is very careful about sharing his own Personal Information and has never knowingly transmitted unencrypted Personal

Information over the internet or any other unsecured source. Plaintiff Lively is diligent about keeping hard copy documents containing Personal Information secure, and is diligent about the online security of his accounts.

138. Plaintiff **Natasha McIntosh** is a citizen of Alabama residing in Brockton. Plaintiff McIntosh was a customer of Boost Mobile from 2002 to 2022 and was an employee of Boost Mobile for a year, starting around 2003. She provided Boost Mobile with at least her name, SSN, email, and payment card information.

139. After the Data Breach began, in the spring of 2024, Plaintiff McIntosh received a notice that an unauthorized party had opened an account with a furniture store using her name and phone number. She started to receive calls and texts about repossessions of furniture that she never bought.

140. Plaintiff McIntosh has been informed that her personal information was found on the dark web. Since the Data Breach, Plaintiff McIntosh has experienced an increase in spam and receives approximately 50 spam calls or messages a day. Since the Data Breach, Plaintiff McIntosh has spent countless hours investigating and mitigating against the substantial risks presented by the theft of her Personal Information. These mitigation efforts have included freezing her credit with credit agencies, registering for credit monitoring services, and monitoring her credit accounts and reports.

141. As a result of the Data Breach, Plaintiff McIntosh has suffered injury and damages, including but not limited to, the unauthorized use of her stolen Personal Information; the substantial risk of identity theft and reasonable mitigation efforts spent to protect against such risks, including time and expenses spent obtaining credit monitoring services and reviewing financial accounts for fraudulent activity; loss of property and value of that property with respect to the inability to control use of her Personal Information; invasion of her privacy; and emotional distress and anxiety resulting from the theft of her Personal Information and responding to identity theft.

142. Plaintiff McIntosh is very careful about sharing her own Personal Information and has never knowingly transmitted unencrypted Personal Information over the internet or any other unsecured source. Plaintiff McIntosh is diligent about keeping hard copy documents containing Personal Information secure, and is diligent about the online security of her accounts.

143. **Plaintiff Debby Worley** is a citizen of New Jersey residing in Clifton. Plaintiff Worley has been a Boost Mobile customer for approximately two to three years. Boost Mobile is an MVNO of AT&T and its customers, like Plaintiff Worley, suffered from the Data Breach in part as a result of Boost Mobile's use of AT&T's network.

144. Plaintiff Worley received a notice letter from Boost Mobile dated November 18, 2024. Since the Data Breach, Plaintiff Worley has experienced an increase in spam and scam phone calls probing her for information. Since the Data Breach, Plaintiff Worley has spent approximately 10 hours investigating and mitigating against the substantial risks presented by the theft of her Personal Information. Without guidance from AT&T or Boost Mobile, her mitigation efforts have been reasonable, including monitoring her credit accounts and reports, changing her passwords, and researching the breach.

145. As a result of the Data Breach, Plaintiff Worley has suffered injury and damages, including but not limited to, the unauthorized use of her stolen Personal Information; the substantial risk of identity theft and reasonable mitigation efforts spent to protect against such risks, including time and expenses spent reviewing financial accounts for fraudulent activity; loss of property and value of that property with respect to the inability to control use of her Personal Information; invasion of her privacy; and emotional distress and anxiety resulting from the theft of her Personal Information and responding to identity theft.

146. Plaintiff Worley is very careful about sharing her own Personal Information and has never knowingly transmitted unencrypted Personal Information over the internet or any other unsecured source. Plaintiff Worley is

diligent about keeping hard copy documents containing Personal Information secure, and is diligent about the online security of her accounts.

JURISDICTION AND VENUE

147. This Representative Class Action Complaint is filed pursuant to the Court's Case Management Order Regarding Form of the Complaint, Order of Preliminary Motions, and Initial Disclosures (Doc. No. 285).

148. The transferor courts have subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, and Defendants are citizens of States different from that of at least one Class member. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

149. Venue is proper in this District for pretrial purposes consistent with the process for multidistrict litigation for the reasons set out in the Judicial Panel on Multidistrict Litigation's Transfer Order centralizing actions consolidated in this MDL to the District of Montana. *In re: Snowflake, Inc. Data Sec. Breach Litig.*, MDL No. 3126, 2024 WL 4429233 (J.P.M.L. 2024). Venue is appropriate in the transferor courts for the reasons stated in Plaintiffs' underlying complaints.

150. Each individual Plaintiff in this action has filed an underlying action which has already either been transferred to this Court for pretrial treatment, or will soon be transferred to this Court for pretrial treatment.

FACTUAL ALLEGATIONS

PART ONE: THE DATA BREACH

151. Snowflake is one of the largest data storage providers in the United States and it contracts with thousands of organizations around the world to securely store their consumer and employee data on its "Data Cloud" platform.[21] Snowflake's platform is a product and a service that provides companies the ability to store, process, and analyze large volumes of consumer and employee data.[22]

152. Snowflake's product is typically referred to as "Software as a Service" (SaaS), which refers to the fact that Snowflake's software allows its customers to connect to cloud-based applications over the internet.

153. Each of the Spoke Defendants is a Snowflake customer and stores consumer and/or employee Personal Information on the Data Cloud.

---

[21] Snowflake, *How It All Started*, https://www.snowflake.com/en/company/overview/about-snowflake/ (last visited Jan. 6, 2025).

[22] Snowflake, *The Snowflake Platform*, https://www.snowflake.com/en/data-cloud/platform/ (last visited Jan. 6, 2025).

I. Multiple, basic cybersecurity failures led to the Data Breach.[23]

154. The events leading up to the Data Breach and its fallout are summarized in a June 10, 2024 report published by Mandiant (the "Mandiant Report"), a cybersecurity firm that assisted Snowflake in its investigation of the Data Breach.[24]

155. Beginning on or around April 2024, a cybercriminal group named UNC5537 carried out a successful cyberattack on Snowflake, exfiltrating the data of hundreds of Snowflake customers, including the Spoke Defendants.

156. UNC5537 is a known cybercriminal group likely comprised of hackers in North America. A financially motivated threat actor, UNC5537 employs information-stealing malware to infiltrate systems, collect user data, exfiltrate that

---

[23] Additional details regarding the breach will be revealed through discovery, including information related to a report prepared by another, reputable cybersecurity company, which was demanded to be taken off the internet by Snowflake. *See* Part Two, *infra*.

[24] Mandiant, *UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion*, Google Cloud (June 10, 2024), https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion (cited to hereinafter as "*Mandiant Report*"). Since Snowflake had a hand in the *Mandiant Report*, the events are likely worse than presented, and will be clarified in discovery. *See also Snowflake Breach: Hacker Confirms Access Through Infostealer Infection*, Hudson Rock, https://archive.is/tljkW ("Hudson Rock Report," archived website).

data, and then sell it on underground cybercrime forums or sell the information to other hackers.[25]

157. UNC5537's successful cyberattack on Snowflake and the Spoke Defendants was simple and easily prevented. As the Mandiant Report put it, the cyberattack was "not the result of any particularly novel or sophisticated tool, technique, or procedure" but was the consequence of "missed opportunities" on the part of Snowflake and the Spoke Defendants to properly secure their credentials.[26]

158. UNC5537's cyberattack boiled down to two basic steps. First, UNC5537 gained access to a customer's Snowflake credentials—i.e., their username and password. Stolen credentials are common and represent a well-known and easily anticipated risk by cybersecurity companies.[27] According to the Mandiant Report, UNC5537 was also "likely able to aggregate credentials" for a large number Snowflake customers by simply perusing various sources of

---

[25] UNC5537 Summary, Mphasis (June 17, 2024), https://www.mphasis.com/content/dam/mphasis-com/global/en/home/services/cybersecurity/june-17-19-unc5537.pdf.

[26] *Mandiant Report*, *supra* n. 24.

[27] *See* TJ Alldridge, *Stolen Credentials Make You Question Who Really Has Access*, Mandiant (Feb. 13, 2024), https://cloud.google.com/blog/products/identity-security/stolen-credentials-make-you-question-who-really-has-access ("stolen credentials are the third most used infection vector behind exploits and phishing").

previously stolen credentials, as "large lists of stolen credentials exist both for free and for purchase inside and outside of the dark web."[28]

159. Next, UNC5537 simply used the stolen credentials to login to a Snowflake customer's account and exfiltrate customer data.[29]

160. According to the Mandiant Report, the success of UNC5537's straightforward cyberattack was made possible by "three primary factors" on the part of Snowflake and the Spoke Defendants.[30]

161. **First**, the affected customers did not have MFA enabled, nor did Snowflake require them to have it enabled. MFA is a basic and industry-standard cybersecurity measure, available for nearly three decades,[31] that requires a user to, in addition to providing their username and password, further authenticate their identity through another source, such as through a passcode sent by text message or

---

28 *Mandiant Report*, *supra* n. 24.

29 *Id.*

30 *See also* Brad Jones, Detecting and Preventing Unauthorized User Access, Snowflake (June 2, 2024), Detecting and Preventing Unauthorized User Access - Cybersecurity - Snowflake (Snowflake recommending MFA, trusted locations, and resetting credentials).

31 Bojan Šimić, *Identity in the Digital Age and the Rise of Multi-Factor Verification*, Forbes (Oct. 10, 2024), https://www.forbes.com/councils/forbestechcouncil/2024/10/10/identity-in-the-digital-age-and-the-rise-of-multi-factor-verification/ (MFA was developed by AT&T as a system to exchange codes on two-way pagers).

email.[32] Without MFA, a valid username and password was all UNC5537 needed to access a Snowflake customer's data—similar to a key placed under a doormat.

162. Strikingly, even though the federal government has urged companies to use MFA to secure data since 2016,[33] and Snowflake offered "free and available" MFA to customers since June 2015,[34] at the time of the Data Breach, Snowflake's default setting turned off MFA. Moreover, Snowflake customers did not have the ability to require their users to use MFA.

163. Snowflake later changed these policies, but not until after the Data Breach. On July 9, 2024, Snowflake announced that customers could now enforce MFA for its users and monitor MFA compliance.[35] And on September 13, 2024, Snowflake announced a new policy which, for the first time, established a default

---

[32] Rose de Fremery, *Tracing the Evolution of Multi-Factor Authentication*, LastPass (Oct. 16, 2023), https://blog.lastpass.com/posts/tracing-the-evolution-of-multi-factor-authentication.

[33] *Fact Sheet:* Cybersecurity National Action Plan, The White House (Feb. 9, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

[34] Snowflake Advances Cybersecurity Excellence by Joining CISA Secure by Design Pledge (July 29, 2024), https://www.snowflake.com/en/blog/snowflake-cybersecurity-cisa-secure-by-design/. Snowflake has also used MFA to protect its own systems. Mihir Bagwe, *The Snowballing of the Snowflake Breach: All About the Massive Snowflake Data Breach*, CyberExpress (June 17, 2024), https://thecyberexpress.com/all-about-massive-snowflake-breach/.

[35] Brad Jones & Anoosh Saboori, *Snowflake Admins Can Now Enforce Mandatory MFA*, Snowflake (July 9, 2024), https://www.snowflake.com/en/blog/snowflake-admins-enforce-mandatory-mfa/.

setting *requiring* MFA for users of Snowflake accounts created as of October 2024.[36]

164. **Second,** Defendants did not have policies and procedures in place to rotate or disable stale credentials. Notably, many of the credentials stolen by UNC5537 through malware were old, and were originally stolen through various malware attacks dating as far back to 2020. But without policies in place to rotate or disable such stale credentials, the years-old credentials remained valid and allowed UNC5537 to exfiltrate Snowflake customers' data.

165. Addressing the issue of stolen credentials, Snowflake now advertises that it automatically disables leaked passwords detected on the dark web.[37] This technology is also available to any of the Defendants.

166. **Third,** the affected customers—including the Spoke Defendants—did not restrict access to Snowflake cloud-based storage based upon certain trusted locations. Conditional Access Policies allow companies to fine-tune access to control from which devices and locations users can access resources. Again,

---

[36] Anoosh Saboori & Brad Jones, *Snowflake Strengthens Security with Default Multi-Factor Authentication and Stronger Password Policies*, Snowflake (Sept. 13, 2024), https://www.snowflake.com/en/blog/multi-factor-identification-default/.

[37] Snowflake Will Automatically Disable Leaked Passwords Detected on the Dark Web, Snowflake (Nov. 14, 2024), https://www.snowflake.com/en/blog/leaked-password-protection/.

without such protection, a valid username and password entered was all UNC5537 needed to access a Snowflake customer's data from anywhere at any time.

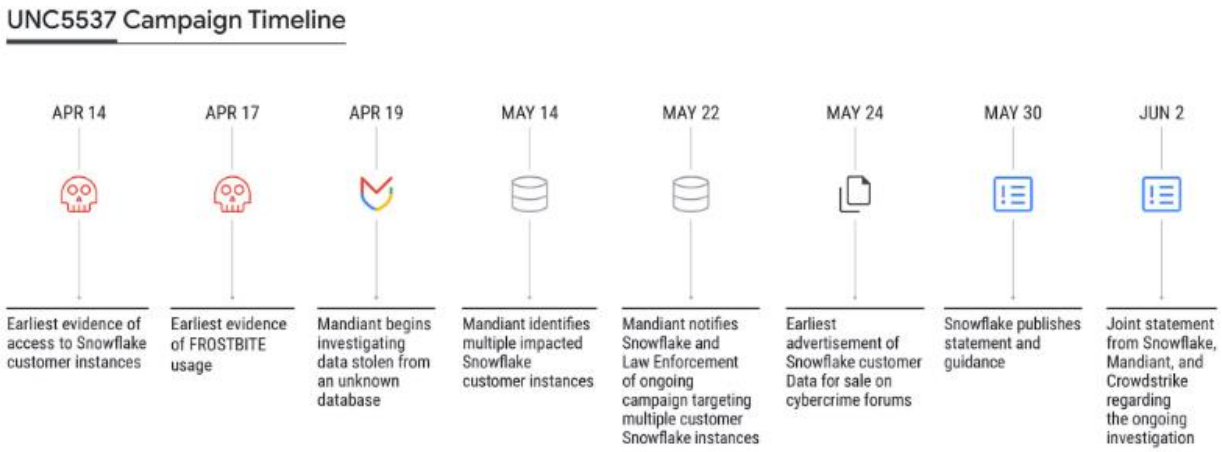
167. On May 30, 2024, Snowflake publicly disclosed the Data Breach for the first time through a blog post authored by CISO Brad Jones, which explained that Snowflake "became aware of potentially unauthorized access to certain customer accounts on May 23, 2024" and was "investigating an increase in cyber threat activity targeting some of our customers' accounts."[38]

168. The Mandiant Report documented the timeline of the Data Breach, which shows a concerning lag in Snowflake's response. As shown in the Mandiant Report timeline provided below, Snowflake did not make a public statement regarding the Data Breach until May 30, 2024. Snowflake's public disclosure came over a month and a half after Mandiant identified evidence of improper access to Snowflake customer data on April 14—but only a week after advertisements for the sale of stolen Snowflake customer data started showing up on cybercrime forums on May 24.[39]

---

[38] Brad Jones, *Detecting and Preventing Unauthorized User Access*, Snowflake (May 30, 2024), https://snowflake.discourse.group/t/detecting-and-preventing-unauthorized-user-access/8967.

[39] *Mandiant Report*, *supra* n. 24.



169. The Mandiant Report further found that UNC5537 was operating "with the intent of data theft and extortion" and was "advertising victim data for sale on cybercrime forums and attempting to extort many of the [customer] victims."[40]

170. As set out in more detail herein, Plaintiffs' and Class Members' Personal Information has already been sold and exchanged on the dark web between UNC5537 and various other cybercriminal threat actors such as Scattered Spider.[41]

171. The Mandiant Report concluded that UNC5537's cyberattack "underscores the urgent need for credential monitoring, the universal enforcement of MFA and secure authentication, limiting traffic to trusted locations for crown

40 *Id.*

41 SC Staff, *Ransom demands issued to Snowflake hack victims*, SC Media (June 18, 2024), https://www.scworld.com/brief/ransom-demands-issued-to-snowflake-hack-victims.

jewels, and alerting on abnormal access attempts."[42] Credential monitoring, MFA, limiting access, and alerts are all ubiquitous cybersecurity practices that have been standard for years.

II. Relevant industry standards and regulations for data security were not followed by Defendants.[43]

A. The Federal Trade Commission's straightforward guidelines were not followed.

172. The Federal Trade Commission ("FTC") has issued guidance and taken enforcement actions that together illustrate the data security industry standards applicable to Snowflake and the Spoke Defendants.

173. Indeed, the FTC's enforcement actions have established that a company's failure to maintain reasonable and appropriate data security of consumer Personal Information violates the FTC Act's prohibition on "unfair or deceptive acts."[44]

---

[42] *Mandiant Report*, *supra* n. 24.

[43] The below recitation of information security standards only provides an introduction as to applicable guidance. *See, e.g.,* NIST Update: Multi-Factor Authentication and SP 800-63 Digital Identity Guidelines, Federal Cybersecurity and Privacy Forum (Feb. 15, 2022), https://csrc.nist.gov/csrc/media/Presentations/2022/multi-factor-authentication-and-sp-800-63-digital/images-media/Federal_Cybersecurity_and_Privacy_Forum_15Feb2022_NIST_Update_Multi-Factor_Authentication_and_SP800-63_Digital_Identity_%20Guidelines.pdf.

[44] *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 244-47 (3d Cir. 2015); Isabella Wright and Maia Hamin, *"Reasonable" Cybersecurity in Forty-Seven Cases: The Federal Trade Commission's Enforcement Actions*

174. In 2016, the FTC published guidance titled, *Protecting Personal Information: A Guide for Business* (the "FTC 2016 Guidance").[45] The FTC 2016 Guidance:

- Stresses the importance of "[c]ontrol[ling] access to sensitive information" and expressly encourages businesses to "[c]onsider using multi-factor authentication, such as requiring the use of a password and a code sent by different methods."[46]
- Emphasizes that companies should respond appropriately when credentials are compromised, providing that businesses should "[r]equire password changes when appropriate—for example, following a breach."[47]
- Instructs companies to restrict data access privileges by "[s]cal[ing] down access to data" and ensuring that "each employee should have access only to those resources needed to do their particular job."[48]
- Warns companies that their data security practices depend on their personnel, which "includ[e] contractors" and encourages companies to "investigate [contractor] data security practices and compare their standards" and "verify compliance" with written security expectations.[49]

Against Unfair and Deceptive Cyber Practices, DFR Lab (June 12, 2024), https://dfrlab.org/2024/06/12/forty-seven-cases-ftc-cyber/.

45 *Protecting Personal Information: A Guide for Business*, Fed. Trade Comm'n (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business ("The FTC 2016 Guidance").

46 *Id.* at 13.

47 *Id.*

48 *Id.* at 7.

49 *Id.* at 27.

- Recommends companies encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems and respond to security incidents.[50]

- Advises companies not to maintain Personal Information longer than necessary, not to collect more Personal Information than necessary, to use industry-tested methods for data security, and monitor and respond to suspicious activity.[51]

175. In 2021, the FTC amended its "Safeguards Rule" that applies to financial institutions, including retailers that issue their own credit card to consumers and companies that bring together buyers and sellers of products and services.[52] The Safeguard Rule requires covered businesses to "[i]mplement multi-factor authentication for anyone accessing customer information on [the business's] system," to "[i]mplement and periodically review access controls [to] [d]etermine who has access to customer information and reconsider on a regular basis whether they still have a legitimate business need for it," and to "[i]mplement procedures and controls to monitor when authorized users are accessing customer information on your system and detect unauthorized access."[53]

---

50 *Id.* at 9-11.

51 *Id.* at 6-22.

52 FTC Safeguards Rule, 86 Fed. Reg. 707272-01, 70305-06 (Dec. 9, 2021) (to be codified at 16 C.F.R. § 314.2(h)(2)(i), (xiii)).

53 *FTC Safeguards Rule: What Your Business Needs to Know*, Fed. Trade Comm'n, https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know (last visited Jan. 7, 2025).

176. In February 2023, the FTC published an article titled, *Security Principles: Addressing underlying causes of risk in complex systems.* The article highlighted the importance of MFA, stating: "Multi-factor authentication is widely regarded as a critical security practice because it means a compromised password alone is not enough to take over someone's account."[54]

177. The FTC's enforcement actions over the past five years further emphasize the critical and fundamental role MFA plays in an effective data security system, where the FTC has repeatedly obtained MFA as a form of injunctive relief in data security enforcement actions.[55]

178. The FTC has also issued guidance for businesses regarding how to respond to data breaches, titled *Data Breach Response: A Guide for Business* (the "FTC Response Guidance"). The FTC Response Guidance stresses the importance of providing individuals affected by a data breach with notice, explaining: "If you quickly notify people that their personal information has been compromised, they

---

[54] Alex Gaynor, *Security Principles: Addressing underlying causes of risk in complex systems*, Fed. Trade Comm'n (Feb. 1, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/02/security-principles-addressing-underlying-causes-risk-complex-systems.

[55] *FTC v. Equifax, Inc.*, No. 1:19-CV-03297, 15 (N.D. Ga. July 23, 2019) (Stipulated Order); *In re Chegg, Inc.*, 2023151 FTC C-4782, 5 (Jan. 25, 2023) (Order); *In re Drizly, LLC*, 2023185 FTC C-4780, 6 (Jan. 9, 2023) (Order).

can take steps to reduce the chance that their information will be misused."[56] The guidance emphasizes that businesses should "[c]learly describe what you know about the compromise" and include "what information was taken." Notifying individuals as to the type of information that was compromised in the breach provides key information that allows them to "take steps to limit the damage."[57]

179. Specific to cloud-storage applications, in June 2020, the FTC published an article titled, *Six steps toward more secure cloud computing.* The article warned, "[a]s cloud computing has become business as usual for many businesses, frequent news reports about data breaches and other missteps should make companies think carefully about how they secure their data." The article expressly highlights the importance of MFA in protecting consumer data stored on cloud services, recommending that businesses: "Require multi-factor authentication and strong passwords to protect against the risk of unauthorized access."[58]

---

56 *Data Breach Response: A Guide for Business*, Fed. Trade Comm'n (Feb. 2021), https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business ("FTC Response Guidance").

57 *Id.*

58 Elisa Jillson & Andy Hasty, *Six steps toward more secure cloud computing*, Fed. Trade Comm'n (June 15, 2020), https://www.ftc.gov/business-guidance/blog/2020/06/six-steps-toward-more-secure-cloud-computing.

180. In March 2023, the FTC issued a Request for Information seeking public comment on "Business Practices of Cloud Computing Providers that Could Impact Competition and Data Security."[59] After reviewing over 100 public comments on the issue, the FTC published a report in November 2023 titled, *Cloud Computing RFI: What we heard and learned.*[60] The report expressly flagged the room for improvement in cloud security as follows: "[A] a number of commenters argued there is a great deal of room for improvement in cloud security; that default security configurations could be better; and that the 'shared responsibility' model for cloud security often lacks clarity, which can lead to situations where neither the cloud provider nor the cloud customer implements necessary safeguards."[61]

B. Payment Card Industry Data Security Standards were not followed.

---

59 *Solicitation for Public Comments on the Business Practices of Cloud Computing Providers*, Fed. Trade Comm'n (Mar. 22, 2023), https://www.regulations.gov/docket/FTC-2023-0028/document.

60 Nick Jones, *Cloud Computing RFI: What we heard and learned*, Fed. Trade Comm'n (Nov. 16, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/11/cloud-computing-rfi-what-we-heard-learned.

61 *Id.* Snowflake used this "shared responsibility" model. *What We Know So Far about the Snowflake "Breach,"* Symmetry Systems (Nov. 6, 2024), https://www.symmetry-systems.com/blog/what-we-know-so-far-about-the-snowflake-breach/ ("Despite the high-profile nature of the breaches and the potential reputational risk, Snowflake has not deviated from the shared responsibility model.").

181. The Payment Card Industry Data Security Standards ("PCI DSS") is an information security standard applicable to the storage of payment card information whose use is mandated by major credit card brands. The PCI DSS is developed and issued by the Payment Card Industry Security Standards Council, which describes itself as a "global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection."[62]

182. The PCI DSS applies to companies like Snowflake and the Spoke Defendants that accept, process, or store credit card information.

183. The PCI DSS reiterates many of the recommendations provided by FTC guidance.

184. As to multifactor authentication, PCI DSS Requirement 8.3 requires: "Secure all non-console administrative access and remote access to the cardholder data environment using multi-factor authentication."[63]

---

[62] PCI, *Who We Are*, https://www.pcisecuritystandards.org/about_us/ (last visited Jan. 7, 2025).

[63] PCI, *PCI DSS Quick Reference Guide*, 19 (July 2018), https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf. *See also* Frederik Mennes, *PCI DSS 4.0: New multi-factor authentication requirements*, OneSpan (May 23, 2024), https://www.onespan.com/blog/new-mfa-requirements-in-PCI-DSS-4.0 (noting in requirements 8.4.2 and 8.5 additional configuration for MFA).

185. The PCI Security Standards Council has issued an April 2018 supplement to the PCI DSS titled, *PCI SSC Cloud Computing Guidelines.*[64] The PCI Cloud Computing Guidelines again emphasize the importance of MFA, providing: "PCI DSS Requirement 8.2.2 requires multi-factor authentication for all remote network access to the CDE [cardholder data environment], and when public cloud services are part of a Customer's CDE, all such access will be considered remote access and will require multi-factor authentication."[65]

186. PCI DSS Requirements 7.1 and 7.2 stress the need to restrict data access privileges, requiring businesses to "[l]imit access to system components and cardholder data to only those individuals whose job requires such access" and "[e]stablish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to 'deny all' unless specifically allowed."[66]

187. The PCI SSC Cloud Computing Guidelines includes a section titled *Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS)*, which provides: "As the Customer's access to network level data can be severely restricted

---

64 PCI Security Standards Council & Cloud Special Interest Group, *PCI SSC Cloud Computing Guidelines* (April 2018), https://listings.pcisecuritystandards.org/pdfs/PCI_SSC_Cloud_Guidelines_v3.pdf.

65 *Id.* at 77.

66 PCI, *PCI DSS Quick Reference Guide*, *supra* n. 63 at 18-19.

in cloud environments, the responsibility for tracking intrusions at the network layer will often reside with the Provider, as the only entity that has sufficient privileges to do this across the underlying infrastructure."[67] The guidelines go on to note that for SaaS providers such as Snowflake: "Since customer access to low level network traffic is impossible, it must rely on Providers for IDS/IPS, monitoring and alerting."[68]

188. The PCI DSS includes the following requirements and recommendations that mirror the FTC's guidance on data retention, data encryption, monitoring data access, and implementing data security policies.[69]

- **Requirement 1.2.** "Build firewall and router configurations that restrict all traffic, inbound and outbound, from "untrusted" networks (including wireless) and hosts, and specifically deny all other traffic expect for protocols necessary for the cardholder data environment."
- **Requirement 3.1.** "Limit cardholder data storage and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in your data retention policy. Purge unnecessary stored data at least quarterly."
- **Requirement 4.** "Encrypt transmission of cardholder data across open, public networks."
- **Requirement 10.** "Regularly Monitor and Test Networks . . . To prevent exploitation, organizations must regularly monitor and test networks to find and fix vulnerabilities"

---

67 PCI, *PCI SSC Cloud Computing Guidelines*, *supra* n. 64 at 63.

68 *Id.*

69 PCI, *PCI DSS Quick Reference Guide*, *supra* n. 63 at 12-16, 21-25.

- **Requirement 10.6.** "Review [audit] logs and security events for all system components to identify anomalies or suspicious activity. Perform critical log reviews at least daily."

- **Requirement 12.1.** "Establish, publish, maintain, and disseminate a security policy; review the security policy at least annually and update when the environment changes.

- **Requirement 12.2.** "Implement a risk assessment process that is performed annually and upon significant changes to the environment that identifies critical assets, threats, and vulnerabilities, and results in a formal assessment."

- **Requirement 12.10.** "Implement an incident response plan. Be prepared to respond immediately to a system breach."

C. Other standards applicable to cloud storage were not followed.

189. In addition to the general data security standards described above, several authorities have issued guidance specific to cloud data storage, defining the roles and responsibilities of cloud service providers (like Snowflake) and customers (like the Spoke Defendants).

190. The Center for Internet Security ("CIS") is a non-profit organization that develops globally recognized best practices for securing IT systems and data. In March 2022, CIS issued a publication titled, *CIS Controls Cloud Companion Guide* that provided guidance as on security best practices for customers using

cloud services.[70] The guidance made the following recommendations emphasizing the importance of MFA and revoking access to stale credentials:

- **Disable Dormant Accounts.** Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.[71]
- **Establish an Access Revoking Process.** Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.[72]
- **Require MFA for Administrative Access.** Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.[73]

191. ISO/IEC 27017 is an international standard that "provides controls and implementation guidance for both cloud service providers and cloud service customers."[74] Control 9.2.3 specifically highlights that cloud service customers

---

70 Center for Internet Security, *CIS Controls Cloud Companion Guide* (Mar. 2022), https://www.cisecurity.org/insights/white-papers/cis-controls-v8-cloud-companion-guide.

71 *Id.* at 18.

72 *Id.* at 20.

73 *Id.*

74 Telecommunication Standardization Sector, *International Standard ISO/IEC 27017*, Int'l Telecomms. Union, 1 (Dec. 15, 2015), https://www.amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027017-2015.pdf.

(like the Spoke Defendants) should use MFA, and cloud service providers (like Snowflake) should provide MFA capabilities as follows[75]:

Cloud service customer	Cloud service provider
The cloud service customer should use sufficient authentication techniques (e.g., multi-factor authentication) for authenticating the cloud service administrators of the cloud service customer to the administrative capabilities of a cloud service according to the identified risks.	The cloud service provider should provide sufficient authentication techniques for authenticating the cloud service administrators of the cloud service customer to the administrative capabilities of a cloud service, according to the identified risks. For example, the cloud service provider can provide multi-factor authentication capabilities or enable the use of third-party multi-factor authentication mechanisms.

III. The Data Breach harmed Plaintiffs and Class Members.

192. The effects of the Data Breach were felt immediately—not only by Snowflake and the Spoke Defendants—but by individual consumers. Personal Information is valuable property. Its value is axiomatic, considering the market value and profitability of "Big Data" to corporations in America.[76]

---

75 *Id.* at 9.

76 Illustratively, Alphabet Inc., the parent company of Google, reported in its 2020 Annual Report a total annual revenue of $182.5 billion and net income of $40.2 billion. $160.7 billion of this revenue derived from its Google business, which is driven almost exclusively by leveraging the Personal Information it collects about users of its various free products and services. Alphabet Inc., Annual Report (Form 10-K) at 32 (Feb. 3, 2021), https://www.sec.gov/ix?doc=/Archives/edgar/data/0001652044/000165204421000010/goog-20201231.htm.

193. Criminal law also recognizes the value of Personal Information and the serious nature of the theft of Personal Information by imposing prison sentences for its theft. This strong deterrence is necessary because cybercriminals extract substantial revenue through the theft and sale of Personal Information. Once a cybercriminal has unlawfully acquired Personal Information, the criminal can use the Personal Information to commit fraud or identity theft or sell the Personal Information to other cybercriminals on the black market.

194. Information protected by credentials—usernames and passwords—is intended to stay private, and not to be disclosed to third parties (otherwise, why password-protect the information, at all?). But because of Defendants' failure to follow basic cybersecurity guidelines, the information stored on Snowflake's cloud-based servers was accessible to cybercriminals, who exfiltrated the data for nefarious purposes.

195. Each of the Spoke Defendants has disclosed that certain types of Personal Information were exposed in the Data Breach. They include, at a minimum:

- **Advance Auto**: Information collected from individuals as part of the employment application process, including Social Security

numbers, driver's license or other government issued identification numbers, and dates of birth.[77]

- **Ticketmaster**: consumer name, contact information, and encrypted credit card information.[78]

- **LendingTree**: customer contact information (names and addresses), driver's license number.[79]

- **AT&T**: records of calls and text of nearly all of AT&T's cellular customers, customers of other companies using AT&T's wireless network, and AT&T's landline customers who interacted with cellular numbers between May 1, 2022 and October 31, 2022. The information also contains records from January 2, 2023, for a small number of customers.[80]

196. The Personal Information exposed is extremely valuable and can be used for a number of nefarious purposes.

A. Sale of the Snowflake information on the dark web and to other criminals.

---

[77] Advance Stores Company, Incorporated, Notice of Data Breach (July 10, 2024), https://consumer.sc.gov/sites/consumer/files/Documents/Security%20Breach%20Notices/AdvanceStoresCompanyInc.pdf ("Advance Auto Notice").

[78] Ticketmaster Data Security Incident, https://help.ticketmaster.com/hc/en-us/articles/26110487861137-Ticketmaster-Data-Security-Incident.

[79] QuoteWizard Notice of Data Breach (July 30, 2024) ("QuoteWizard Notice"), https://ago.vermont.gov/sites/ago/files/documents/2024-08-09%20QuoteWizard%20Data%20Breach%20Notice%20to%20Consumers.pdf.

[80] AT&T Addresses Illegal Download of Customer Data, AT&T (July 12, 2024) ("AT&T Notice"), https://about.att.com/story/2024/addressing-illegal-download.html.

197. First, cybercriminals have already confirmed the stolen Personal Information's value by selling the data on the dark web and to other cybercriminals.

198. Some dark web sites are simply places for people who wish to avoid tracking while browsing the internet.[81] However, the anonymity of the dark web has led to the creation of a number of markets and forums which traffic in illegal merchandise and content, including stolen Personal Information.[82]

199. The dark web is a heavily cloaked part of the internet that makes it difficult for authorities to detect the location or owners of a website. The dark web is not indexed by normal search engines such as Google and is only accessible using a Tor browser (or similar tool), which aims to conceal users' identities and online activity. The dark web is notorious for hosting marketplaces selling illegal items such as weapons, drugs, and Personal Information. Websites appear and disappear quickly, making it a dynamic environment.

---

81 Thomas J. Holt, *Open, Deep, and Dark: Differentiating the Parts of the Internet Used For Cybercrime*, Mich. State Univ., https://cj.msu.edu/_assets/pdfs/cina/CINA-White_Papers-Holt_Open_Deep_Dark.PDF (last visited Nov. 26, 2024).

82 *Crime and the Deep Web*, Stevenson Univ., https://www.stevenson.edu/online/about-us/news/crime-deep-web/ (last visited Nov. 26, 2024); *Defending Against Malicious Cyber Activity Originating from Tor*, CISA, https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-183a (last updated Aug. 2, 2021).

200. Once stolen Personal Information is posted on the dark web, it will most likely be distributed or sold to multiple different groups and individuals, each of which can use that information for fraud and identity theft.[83]

201. When data is stolen, it can appear on the dark web across the world. In 2015, researchers created a list of 1,568 phony names, Social Security numbers, credit card numbers, addresses, and phone numbers, rolled them in an Excel spreadsheet, and then "watermarked" it with their code that silently tracks any access to the file.[84] The data was quickly spread across five continents: North America, Asia, Europe, Africa, and South America. In the end, it was downloaded by 47 different parties. It was mainly downloaded by users in Nigeria, Russia, and

---

83 *The Dark Web and Cybercrime*, HHS (July 23, 2020), https://www.hhs.gov/sites/default/files/dark-web-and-cybercrime.pdf; Lawrence Abrams, *Scam PSA: Ransomware gangs don't always delete stolen data when paid*, BleepingComputer (Nov. 4, 2020), https://www.bleepingcomputer.com/news/security/scam-psa-ransomware-gangs-dont-always-delete-stolen-data-when-paid/.

84 Kelly Jackson Higgins, *What Happens When Personal Information Hits The Dark Web*, DARKREADING (Apr. 7, 2015), https://www.darkreading.com/cyberattacks-data-breaches/what-happens-when-personal-information-hits-the-dark-web; Kristin Finklea, *Dark Web*, Nat'l Sec. Archive (July 7, 2015), https://nsarchive.gwu.edu/media/21394/ocr; *Dark Web*, Congressional Research Service, https://crsreports.congress.gov/product/pdf/R/R44101 (last updated Mar. 10, 2017).

Brazil, with the most activity coming from Nigeria and Russia.[85] This experiment demonstrated that data released on the dark web will quickly spread around the world.

202. Information from this Data Breach has already been found in several places on the dark web—even reappearing after law enforcement agencies shut down certain websites offering information for sale.[86]

203. In a hub-and-spoke breach such as this one, when information from one "spoke" defendant appears on the dark web, it is likely that information from other defendants is likely to follow or has already been sold.

204. The information found for sale on the dark web is just the tip of the iceberg. The dark web poses significant challenges to cyber security professionals and law enforcement agencies. The dark web is legal to access and operate, and it has some legitimate applications and sites. But its hidden nature and its employment

---

85 Pierluigi Paganini, *HOW FAR DO STOLEN DATA GET IN THE DEEP WEB AFTER A BREACH?*, Security Affairs (Apr. 12, 2015), https://securityaffairs.com/35902/cyber-crime/propagation-data-deep-web.html.

86 *See, e.g.*, Ionut Arghire, *Hackers Boast Ticketmaster Breach on Relaunched BreachForums*, SecurityWeek (May 31, 2024), https://www.securityweek.com/hackers-boast-ticketmaster-breach-on-relaunched-breachforums/; Sergiu Gatlan, *Advance Auto Parts stolen data for sale after Snowflake attack*, Bleeping Computer (June 5, 2024), https://www.bleepingcomputer.com/news/security/advance-auto-parts-stolen-data-for-sale-after-snowflake-attack/.

of multi-level encryption make detecting and monitoring illegal activity difficult. Unlike the clear web, dark web sites do not advertise their existence.

B. There are long-lasting impacts of the Data Breach.

205. The U.S. Government Accountability Office (GAO) released a report in 2007 regarding data breaches, finding that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[87]

206. The GAO Report explains that "[t]he term 'identity theft' is broad and encompasses many types of criminal activities, including fraud on existing accounts—such as unauthorized use of a stolen credit card number—or fraudulent creation of new accounts—such as using stolen data to open a credit card account in someone else's name." The GAO Report notes that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[88]

---

87 Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown ("GAO Report") at 2, GAO (June 2007), https://www.gao.gov/assets/270/262899.pdf.

88 *Id*.

207. Identity thieves use Personal Information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[89] According to Experian, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to, among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; or use the victim's information in the event of arrest or court action.[90]

208. With access to an individual's Personal Information, criminals can commit all manner of fraud, including obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and Social Security number to obtain government benefits; filing a

---

89 The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things: "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id*.

90 *See* Louis DeNicola, *What Can Identity Thieves Do with Your Private Information and How Can You Protect Yourself*, Experian (May 21, 2023), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

fraudulent tax return using the victim's information; or committing healthcare fraud using an individual's identification. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[91]

209. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[92]

210. Theft of Social Security numbers creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new Social Security number, a breach victim has to demonstrate ongoing harm from misuse of their Social Security number, and a new Social Security number will not be provided until after the harm has already been suffered by the victim.

211. Due to the highly sensitive nature of Social Security numbers, theft of Social Security numbers in combination with other data (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. Data security researcher Tom Stickley, who is employed by companies to find flaws in

---

91 *Id.*

92 *Id.*

their computer systems, stated: "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[93]

212. A Data Breach does not need to expose Social Security numbers in order to expose victims to actual or concrete harm. For example, there have been numerous examples of victims of "SIM swap" fraud, where criminals essentially "take over" a victim's cell phone number in order to obtain that victim's text messages, break into the victim's accounts, and empty their life's savings. Some criminals have been able to successfully commit a SIM swap with only a victim's name and cellular number. Cellular companies do not necessarily put extra precautions in place to protect individuals from SIM-swap attacks—requiring consumers to understand the risk that such leaked information causes and request a special passcode on their accounts for additional protection.[94]

---

[93] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, Time (Aug. 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

[94] Donie O' Sullivan, *One man lost his life savings in a SIM hack. Here's how you can try to protect yourself*, CNN (Mar. 13, 2020), https://www.cnn.com/2020/03/13/tech/sim-hack-million-dollars/index.html; *FBI warns of growing SIM-swapping threat*, Honolulu Star-Advertiser (Feb. 9, 2022), https://www.yahoo.com/news/fbi-warns-growing-sim-swapping-061700104.html; *UPDATE: Secure Your Number to Reduce SIM Swap Scams*, AT&T, https://www.research.att.com/sites/cyberaware/ni/blog/sim_swap.html (last accessed Jan. 14, 2024); TJ Porter, *Why Sim Swapping Scams Are On The Rise And How You Can Stay Safe*, Investopedia (Dec. 16, 2024), https://www.investopedia.com/protect-yourself-from-sim-swapping-8756219; Dean Reilly, *A Deep Dive into the Tactics Used by Fraudsters*, Hacker Desk

213. Beyond SIM-swap scams, hackers can sell call log information for individuals, exposing sensitive information related to who they have called and when. Indeed, hackers attempted to post call log information from the Data Breach for President Donald Trump and Vice President Kamala Harris.[95] Exposed call records can expose individuals to harassment, identity theft, and other fraud.[96]

214. Recent reports suggest that detailed call logs can also be used to more effectively train malicious artificial intelligence (AI) models to help these models learn specific patterns of communication and movement. By analyzing communication patterns, this AI can craft highly personalized phishing messages that are more likely to succeed, especially if it can identify the parties involved and the nature of the relationship.[97]

(Aug. 4, 2023), https://hackerdesk.com/unmasking-the-sim-swap-scam-a-deep-dive-into-the-tactics-used-by-fraudsters.

[95] Jessica Lyons, *US Army soldier who allegedly stole Trump's AT&T call logs arrested*, The Register (Jan. 1, 2025), https://www.msn.com/en-us/news/crime/us-army-soldier-who-allegedly-stole-trumps-at-t-call-logs-arrested/ar-AA1wNlhv.

[96] Amanda Hetler, *AT&T data breach: What's next for affected customers?*, TechTarget (Jul. 24, 2024), https://www.techtarget.com/WhatIs/feature/ATT-data-breach-Whats-next-for-affected-customers.

[97] David Michael Berry, *How Data Breaches Empower Malicious AI: The AT&T Case Study*, Berry Networks (July 16, 2024), https://berry-networks.com/2024/07/16/how-data-breaches-empower-malicious-ai-the-att-case-study/.

215. Hackers can also use information related to a customer's prior purchase history to perpetrate phishing attacks and scams by sending existing customers fake order confirmations to steal additional personal and financial information.[98]

216. Exposed driver's license numbers are sold on the dark web because they can be used to create counterfeit licenses, open financial accounts, cash counterfeit checks, and even obtain medical care using someone's identity.[99]

217. Exposed gift cards can result in their balances being reduced to nothing—a real and serious loss of monetary value.[100] Individuals may also experience theft of their event tickets.[101]

---

98 *See, e.g.*, *How to avoid scams impersonating Amazon this holiday season*, Amazon (Nov. 17, 2022), https://www.aboutamazon.in/news/amazon-india-news/how-to-avoid-scams-impersonating-amazon-this-holiday-season; *How to Recognize and Avoid Phishing Scams*, FTC (Sept. 2022), https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams.

99 *How driver's licenses exposed in data breaches increase your risk of identity fraud*, IDX (May 6, 2021), https://www.idx.us/knowledge-center/how-drivers-licenses-exposed-in-data-breaches-increase-your-risk-of-identity-fraud; John Egan, *What Should I Do if My Driver's License Number Is Stolen*, Experian (June 13, 2024), https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/.

100 Jackie Callaway, *Beware: Hackers can steal money off gift cards before you have a chance to use them*, ABC News Tampa Bay (Dec. 29, 2020), https://www.abcactionnews.com/money/consumer/taking-action-for-you/beware-hackers-can-steal-money-off-gift-cards-before-you-have-a-chance-to-use-them.

101 Taylor O'Bier, *Hackers allegedly leak tickets from Ticketmaster to Talyor Swift tour and more*, Scripps (Jul. 10, 2024),

218. Each additional piece of Personal Information exposed in a data breach increases an individual's risk of identity fraud and exposure to scams. Information from one breach may be combined with information from other breaches to create "fullz"—or complete information about an individual sufficient to facilitate identity theft, allow for the purchase of goods and services on the internet, and enable criminals to open new accounts in a victim's name.[102]

219. Data breaches also have a deep, psychological impact on their victims. A cyberattack can feel like the digital equivalent of getting robbed, with a corresponding wave of anxiety and dread. Anxiety, panic, fear, and frustration—even intense anger—are common emotional responses when experiencing a

---

https://www.scrippsnews.com/science-and-tech/data-privacy-and-cybersecurity/hackers-allegedly-leak-tickets-from-ticketmaster-to-taylor-swift-tour-and-more ("Sp1d3rHunters hit back, stating in another forum post that the ticket information they allegedly stole was for physical ticket types and therefore they can't be refreshed. If this is true, Ticketmaster would have to void and reissue all the stolen tickets.").

[102] Robert Lemos, *All about your 'fullz' and how hackers turn your personal data into dollars*, PCWorld (June 2, 2016), https://www.pcworld.com/article/414992/all-about-your-fullz-and-how-hackers-turn-your-personal-data-into-dollars.html; Paige Tester, *What are Fullz? How Hackers & Fraudsters Obtain & Use Fullz*, DataDome (Mar. 3, 2023), https://datadome.co/guides/account-takeover/what-are-fullz-how-do-fullz-work/.

cyberattack. While expected, these emotions can paralyze the victim and prolong or worsen the consequences of a cyberattack.[103]

220. The information exposed in this Data Breach will result in actual and imminent harm for Plaintiffs and Class Members for years to come.

C. The data breach forces Plaintiffs and Class Members to take additional steps to mitigate harm.

221. In addition to all the other immediate consequences of the Data Breach, Plaintiffs and Class Members face a substantially increased risk of identity theft and fraud.

222. The FTC recommends that identity theft victims take several steps to protect their Personal Information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and to consider an extended fraud alert that lasts for seven years if identity theft occurs), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[104]

---

[103] Amber Steel, *The Psychological Impact of Cyber Attacks*, LastPass (Aug. 17, 2022), https://blog.lastpass.com/posts/the-psychological-impact-of-cyber-attacks. *See also* Christina Ianzito, *Identity Fraud Cost Americans $43 Billion in 2023*, AARP (Apr. 10, 2024) ("[I]n 2023, 16 percent of identity fraud victims said they'd thought about ending their lives.").

[104] *Identity Theft Recovery Steps*, FTC, https://www.identitytheft.gov/Steps (last visited Nov. 26, 2024).

223. As discussed above, cybercriminals use stolen Personal Information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

224. Studies by the Identity Theft Resource Center ("ITRC") show the multitude of harms caused by fraudulent use of personal and financial information, including needing to request government assistance, borrowing money, using savings to pay for expenses, being unable to qualify for home loans, losing a home or place of residence, being unable to care for one's family, losing an employment opportunity, missing time from work, and needing to take time off of school.[105]

225. Moreover, the harms of identity theft are not limited to the affected individual and may adversely impact other associated persons and support systems, including government assistance programs. In the ITRC study, nearly a quarter of survey respondents had to request government assistance because of identity theft, such as welfare, EBT, food stamps, or similar support systems.[106] The ITRC study concludes that identity theft victimization has an extreme and adverse effect on each

---

105 Jason Steele, *Credit Card and ID Theft Statistics*, Creditcards.com (June 11, 2021), https://www.creditcards.com/statistics/credit-card-security-id-theft-fraud-statistics-1276/; *see also* Identity Theft Resource Center 2023 Consumer Impact Report (Aug. 2023), https://www.idtheftcenter.org/wp-content/uploads/2023/08/ITRC_2023-Consumer-Impact-Report_Final-1.pdf.

106 *Id.*

individual as well as on all of the support systems and people associated with the individual.[107]

226. Personal Information is such an inherently valuable[108] commodity to identity thieves that, once it is compromised, criminals often trade the information on the cyber black-market for years.

227. Accordingly, there may also be a substantial lag time between when harm occurs versus when it is discovered, and also between when Personal Information is stolen and when it is used. According to the GAO Report: "[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[109]

---

107 *Id.*

108 *See, e.g.*, John T. Soma, et al., Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 1, 2 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.").

109 Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown ("GAO Report") at 2, GAO (June 2007), https://www.gao.gov/assets/270/262899.pdf.

228. Furthermore, data breaches that expose any personal data, and in particular non-public data of any kind (e.g., purchase history or call log history), directly and materially increase the chance that a potential victim is targeted by a spear phishing attack in the future, and spear phishing results in a high rate of identity theft, fraud, and extortion.[110]

229. It would be unreasonable for individuals to wait to experience fraud or identity theft before they take steps to protect themselves from fraud or identity theft because of Defendants' negligence or recklessness.

230. The intent of hackers is clear when they hack systems, such as the Defendants': they are attempting to access consumers' Personal Information for malicious purposes, such as selling it for a profit.

---

[110] *See* Leo Kelion & Joe Tidy, *National Trust joins victims of Blackbaud hack*, BBC News (July 30, 2020), https://www.bbc.com/news/technology-53567699 (concluding that personal information such as "names, titles, telephone numbers, email addresses, mailing addresses, dates of birth, and, more importantly, donor information such as donation dates, donation amounts, giving capacity, philanthropic interests, and other donor profile information . . . . in the hands of fraudsters, [makes consumers] particularly susceptible to spear phishing—a fraudulent email to specific targets while purporting to be a trusted sender, with the aim of convincing victims to hand over information or money or infecting devices with malware").

231. On average, it takes approximately three months for a consumer to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information.[111]

232. In addition, there is a strong probability that much of the information stolen in the Data Breach has not yet been made available on the dark web in a coherent, organized fashion, meaning Plaintiffs and Class Members will remain at an increased risk of fraud and identity theft for many years into the future. Plaintiffs and Class Members must vigilantly monitor their financial accounts, online presence, profiles, and other places where their Personal Information may appear for many years to come.

233. Purchasing monitoring products or spending additional time to monitor their Personal Information is a reasonable step to mitigate the risk of harm that Plaintiffs and Class Members face.

D. Defendants failed to protect consumers or compensate victims appropriately.

234. The Defendants in this action did not take sufficient steps to protect their customers, and have not done nearly enough to compensate the victims of the Data Breach, who will suffer real harm for years to come.

---

[111] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

235. As an initial matter, and as discussed herein, Defendants did not implement the most basic of cybersecurity policies that would have prevented the Data Breach. This Data Breach was preventable.[112] Indeed, this is made clear by the number of Snowflake customers who implemented these policies, and did not have their data taken by cybercriminals.

236. The industries that Defendants serve have seen a substantial increase in cyberattacks and data breaches such that they were reckless in not implementing basic cybersecurity practices to protect customer information. Indeed, many of the Defendants have already experienced significant data breaches in recent years such that they could foresee that the Data Breach that is the subject of this action would occur.

237. Cyberattacks have become so notorious that the FBI and Secret Service issued a warning in 2019 to potential targets so that they were made aware of, and could prepare for, a potential attack.[113]

---

[112] Lucy L. Thomson, Data Breach and Encryption Handbook (Am. Bar Assoc. 2011) ("In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions.").

[113] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, Law360 (Nov. 18, 2019), https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

238. There were plenty of technologies and processes readily available that Defendants could have utilized to prevent the Data Breach. Defendants failed to do so. The problem caused by Defendants' unwillingness to take proper data security precautions will only get worse: a study published in May 2022 by the International Data Corporation projects that the amount of new data created, captured, replicated, and consumed is expected to double in size by 2026.[114]

239. The Defendants were on notice of the risks of a data security incident or breach and knew there were steps they could take to secure their systems and protect the Personal Information of their customers; they simply chose not to take them.

240. Additionally, Defendants' actions after the Data Breach have been insufficient, as the Defendants have not offered monitoring tools that would adequately protect victims, nor have they compensated victims for their injuries.

E. Damages can compensate victims for the harm caused by the attack.

241. While several Defendants have offered victims of the Data Breach credit monitoring services, these services alone are not enough: a year or two of credit monitoring will not un-ring the bell of the release of the Personal Information

---

114 *See* John Rydning, *Worldwide IDC Global DataSphere Forecast, 2022–2026: Enterprise Organizations Driving Most of the Data Growth*, IDC (Nov. 2022), https://www.linkedin.com/embeds/publishingEmbed.html?articleId=7080078918768595657.

of Plaintiffs and Class Members, which will circulate through the various levels (clear, dark, and deep) of the internet for years and years, if not in perpetuity. Identity theft and credit monitoring services are insufficient to protect consumers from certain scams, phishing attempts, malware, and additional extortion that they will likely face and have already faced as a result of the breach. Data Breach victims will need to safeguard their information and accounts for years to come—and these services are typically accounted for in settlements and judgments involving data breaches.[115]

242. The Personal Information exposed in the Data Breach has real value, as explained above. Plaintiffs and the Class Members have therefore been deprived of their rights to the control of that property and have lost the value they might otherwise have incurred from that data.[116]

243. Plaintiffs and the Class Members have spent significant time, and will spend more, monitoring their accounts, changing login credentials, and recovering

---

[115] For instance, in July 2019, the CFPB, FTC and States announced a settlement with Equifax over the 2017 Equifax data breach, which included up to ten years of credit monitoring and identity restoration services. *See CFPB, FTC and States Announce Settlement with Equifax Over 2017 Data Breach*, CFPB (July 22, 2019), https://www.consumerfinance.gov/about-us/newsroom/cfpb-ftc-states-announce-settlement-with-equifax-over-2017-data-breach/.

[116] Ravi Sen, *Here's how much your personal information is worth to cybercriminals – and what they do with it*, PBS (May 14, 2021, 12:04 PM), https://www.pbs.org/newshour/science/heres-how-much-your-personal-information-is-worth-to-cybercriminals-and-what-they-do-with-it.

from the inevitable fraud and identity theft which will occur, which deserves to be compensated: Defendants have not made apportionment for this very real injury.[117]

244. Similarly, Defendants have offered no compensation for the aggravation, agitation, anxiety, anguish, loss of dignity, intrinsic harm, and emotional distress that Plaintiffs and the Class Members have suffered, and will continue to suffer, as a result of the Data Breach: the knowledge that their information is out in the open, available for sale and exploitation at any time in the future is a real harm that also deserves compensation.

245. Plaintiffs and Class Members were also deprived of the benefit of their bargain when they interacted with Defendants: each Defendant had a duty to take reasonable steps to protect the Personal Information of its customers. This duty was inherent in the relationships among Plaintiffs and Class Members and Defendants, whether through express contractual terms, implied contractual terms, or statutory or implied duties of good faith and fair dealing.

246. Defendants have not taken sufficient steps or even attempted to make their customers, the real victims of this Data Breach, whole. Defendants have failed

[117] Time spent monitoring accounts is another common and cognizable, compensated harm in data breach cases. *See Equifax Data Breach Settlement*, FTC, https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement (last visited Nov. 26, 2024).

in their duty to protect Plaintiffs' and Class Members' Personal Information and have failed in their duty to help these consumers protect themselves in the future.

247. Plaintiffs who have filed suit in this multidistrict litigation have suffered injuries in numerous ways, including:

- Loss of benefit of their bargain, for individuals who provided compensation to entities to, among other things, safely store their data;
- Loss of economic value of their personal information, in that it has been misused for purposes to which they did not consent, and they have not been properly compensated for this misuse;
- Loss of the privacy of their personal information which has been stolen by cybercriminals and therefore already exposed to the eyes of unauthorized third parties without Plaintiffs' authorization or consent;
- Loss of the intrinsic value of their personal information and the accompanying aggravation, agitation, anxiety, anguish, loss of dignity, and emotional distress;
- Actual or attempted fraud, misuse, or identity theft caused by the Data Breach, including, but not limited to, their information being published to the clear, deep, and dark web; as well as
- Time and expenses that were reasonably spent to mitigate the impact of the breach.

248. Several Plaintiffs have already experienced actual or attempted fraud, which is reasonably related to the Data Breach, which demonstrates that the Data Breach has put them at immediate risk for additional harm.

249. The fraud and attempted fraud that certain Plaintiffs have suffered is sufficiently related to the Data Breach because of the time frame in which it occurred (after the Data Breach), and because the same information that was exposed in the Data Breach would have been used to effectuate the fraud and identity theft.

250. The harm already suffered by Plaintiffs demonstrates that the risk of harm is ongoing for all Plaintiffs and all Class Members.

IV. Alternative forms of dispute resolution that would delay resolution of cases which Defendants sought to consolidate are unconscionable and unenforceable.

251. Alternative forms of dispute resolution, such as mandatory binding arbitration, combined with prohibitions against class actions, are unconscionable and unenforceable in this action.

252. To require all individuals with claims against certain Spoke Defendants to arbitrate their claims, or bring those claims in small claims court, would overwhelm those venues and prevent individuals from having their claims heard for several years.

253. Additionally, certain provisions of such clauses are unconscionable and unenforceable as consumers were unable to negotiate the provisions of their agreements; they were presented on a take-it-or-leave-it basis, and terms were often updated without providing notice to consumers.

PART TWO: SNOWFLAKE

254. All Plaintiffs named in this Representative Complaint pursue claims against Snowflake.

I. Snowflake's business and data security promises.

255. Snowflake is aware and understands that data security is a key feature of the data storage services that it provides to its customers. The following examples illustrate how Snowflake's marketing highlights the strength of its data security practices as a selling point to its customers:

- Snowflake maintains a "Security Hub" webpage that centralizes updates relating to data security. The header of the Security Hub website provides: "Security has been foundational to the Snowflake platform since the very beginning. Our robust security features help you protect your data so you can achieve the results you need."[118]

- The Security Hub website also includes the following quote from Brad Jones, Snowflake's Chief Information Security Officer ("CISO"), emphasizing Snowflake's "industry-leading" data security policies: "Since our founding in 2012, the security of our customers' data has been our highest priority. This unwavering commitment is why we're continuously strengthening our industry-leading, built-in security policies to deliver a trusted experience for our customers. To foster ongoing transparency, we will regularly update this page with the latest security information."[119]

---

118 Snowflake, *Snowflake Security Hub*, https://www.snowflake.com/en/resources/learn/snowflake-security-hub/ (last visited Jan. 6, 2025).

119 *Id.*

- Snowflake also maintains a "Securing Snowflake" website that provides customers with data security guidance. The website represents, "Snowflake provides industry-leading features that ensure the highest levels of security for your account and users, as well as all the data you store in Snowflake."[120]

256. Snowflake is also well aware of industry guidance and regulations that set standards for effective data security practices. Snowflake's marketing repeatedly advertises that its "industry-leading" data security practices enable companies comply with relevant data security standards and regulations.

257. For example, on a webpage titled "Data Security Compliance: Protecting Sensitive Data" (the "Data Security Compliance website"), Snowflake represents: "Snowflake helps organizations streamline security compliance, providing the tools and support required to meet regulatory compliance standards. With industry-leading data security and governance features, organizations can shift their focus from protecting their data to analyzing it."[121]

258. On the Data Security Compliance website, Snowflake further represents how its services enable customers to comply with relevant industry standards and regulations, touting that its services afford customers "[b]aked-in

---

120 Snowflake, *Securing Snowflake*, https://docs.snowflake.com/en/guides-overview-secure (last visited Jan. 6, 2025).

121 Snowflake, *Data Security Compliance: Protecting Sensitive Data*, https://www.snowflake.com/trending/data-security-compliance/ (last visited Jan. 6, 2025).

government and industry data security compliance" and allow for "comprehensive compliance, security and privacy controls that are universally enforced." For example, in a section titled, "How Snowflake Supports Security Compliance," Snowflake represents the following[122]:

- "**Baked-in government and industry data security compliance.** Snowflake has achieved numerous government and industry data security compliance credentials, validating the high level of security required by industries, as well as state and federal governments. Snowflake's government deployments have achieved Federal Risk and Authorization Management Program (FedRAMP) Authorization to Operate (ATO) at the Moderate level along, and support a range of compliance standards: International Traffic in Arms Regulations (ITAR), System and Organization Controls 2 (SOC 2) Type II, PCI DSS and Health Information Trust Alliance (HITRUST)."

- "**Universal governance.** Inconsistent governance policies across systems and users can introduce security risk to your data. Snowflake's single governance model provides comprehensive compliance, security and privacy controls that are universally enforced. Snowflake Horizon unifies and extends data governance resources. With Snowflake Horizon, data teams, data governors and data stewards can leverage a built-in, unified set of compliance, security, privacy, interoperability and access capabilities in the AI Data Cloud. Snowflake Horizon provides the toolkit required to protect and audit data, apps and models with data quality monitoring and lineage. And advanced privacy policies and data clean rooms allow organizations to tap into the full value of their most sensitive data."

259. As one of the nation's largest cloud storage data providers, Snowflake knew or should have known about the importance of implementing effective data

122 *Id.*

security practices to protect Personal Information stored on the Data Cloud, particularly because it held itself out as doing exactly that.

260. Indeed, cloud storage databases are prime targets for cybercriminals due to the sheer volume of data they house. One recent report has highlighted the risks presented by cloud storage as follows[123]:

> It is estimated that more than 60% of the world's corporate data is stored in the cloud. That makes the cloud a very attractive target for hackers. In 2023, over 80% of data breaches involved data stored in the cloud. That is not just because the cloud is an attractive target. In many cases, it is also an easy target due to cloud misconfiguration – that is, companies unintentionally misuse the cloud, such as allowing excessively permissive cloud access, having unrestricted ports, and use unsecured backups

II. Snowflake had a duty to safeguard Plaintiffs' and Class Members' information.

261. Snowflake exists because companies need a company to safeguard their information. The Personal Information of Plaintiffs and Class Members was stored on Snowflake's Data Cloud at the time of the Data Breach by a Spoke Defendant, with whom Snowflake maintained a business relationship to provide data cloud storage services.

262. Snowflake owed a common law duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting,

---

[123] Stuart Madnick, *Why Data Breaches Spiked in 2023*, Harv. Bus. Rev. (Feb. 19, 2024), https://hbr.org/2024/02/why-data-breaches-spiked-in-2023.

and protecting the Personal Information in Snowflake's possession from being compromised, accessed, stolen, or misused by unauthorized parties.

263. Snowflake's duty of reasonable care is consistent with nature of its business, which is to provide secure cloud data services and store massive amounts of data, including Plaintiffs' and Class Members' Personal Information. Snowflake had a duty to exercise reasonable care in safeguarding Plaintiffs' and Class Members' Personal Information, as it was reasonably foreseeable that the failure to do so would cause them injury.

264. Snowflake's duty of reasonable care is established by governmental regulations and industry guidance establishing industry standards for data security to safeguard Personal Information stored on cloud platforms.

265. Snowflake's duty of reasonable care is established by its own marketing statements, which hold out its cloud services as providing "built-in," "baked-in," and otherwise turnkey data security compliance systems.

III. Snowflake breached its duty and engaged in unfair trade practices.

266. Snowflake breached its duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Personal Information by failing to implement adequate data security practices, which caused the Data Breach.

267. Snowflake is well aware of the fact that it is a high-value target for cybercriminals. In March 2023, the FTC sought comments from Computing Providers (like Snowflake) and their impact on end users, customers, companies, and other businesses across the economy (like Spoke Defendants) on the business practices of cloud computing providers including issues related to the market power of these companies, impact on competition, and potential security risks.[124]

268. Despite industry guidance at the time of the Data Breach, while Snowflake permitted customers to use MFA, it required customers to opt in. It did not require MFA, including for specific users in customer environments. Additionally, Snowflake did not provide customers with the ability to enforce MFA on its users—i.e., require users to use MFA.

269. A prominent cybersecurity firm executive described the practical failings of Snowflake's MFA configuration as follows[125]:

> MFA is a critical component in protecting against identity theft, and specifically against attacks related to the successful theft of

---

[124] Press Release, Fed. Trade Comm'n, *FTC Seeks Comment on Business Practices of Cloud Computing Providers that Could Impact Competition and Data Security* (March 22, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-seeks-comment-business-practices-cloud-computing-providers-could-impact-competition-data (last visited Aug. 20, 2024).

[125] Shane Snider, *Snowflake's Lack of MFA Control Leaves Companies Vulnerable, Experts Say*, Information Week (June 5, 2024), https://www.informationweek.com/cyber-resilience/snowflake-s-lack-of-mfa-control-leaves-companies-vulnerable-experts-say.

> passwords through phishing, malware (infostealers), or leakage of reused passwords from compromised sites.
>
> While Snowflake offers users the ability to turn on MFA, this is a feature that is not enabled on users by default and … it cannot be enforced on users by the admin of the tenant. This means Snowflake leaves it up to every user to decide whether they want to enroll with MFA or not. This naturally leads to many Snowflake users not having MFA turned on.
>
> Most SaaS vendors, once deployed as an enterprise solution, allow administrators to enforce MFA … they require every user to enroll in MFA when they first login and make it no longer possible for users to work without it.

270. It was feasible at the time of the Data Breach for Snowflake to allow customers to enforce MFA across their userbase. Indeed, on July 9, 2024—less than a month after disclosing the Data Breach—Snowflake rolled out a "new option" to "help admins enforce usage of MFA" by "requir[ing] MFA for all users in an account." In the announcement, Snowflake touted the enforcement of MFA as a "[b]est practice[]."[126]

271. It was also feasible at the time of the Data Breach for Snowflake to turn on MFA by default, instead of having it turned off. On September 13, 2024—

[126] Brad Jones and Anoosh Saboori, *Snowflake Admins Can Now Enforce Mandatory MFA*, Snowflake (Jul. 9, 2024), https://www.snowflake.com/en/blog/snowflake-admins-enforce-mandatory-mfa/.

just three months after disclosing the Data Breach—Snowflake rolled out another new policy enforcing MFA by default on accounts created as of October 2024.[127]

272. In addition, many of the compromised credentials used by UNC5537 were old and had been acquired from malware campaigns dating back to 2020. Snowflake could have closed off this vulnerability by requiring customers to regularly update their credentials, notifying customers to rotate their credentials accordingly, or monitoring info stealer marketplaces for compromised credentials and blocking access by those credentials (something Snowflake now does).

273. Snowflake also could have prevented the Data Breach by maintaining intrusion detection and prevention systems that notify customers of unusual network traffic, such as a login made by a suspicious credential that could be identified by its last login date. Such a system would be consistent with the PCI Cloud Computing Guidelines, which provides, "Since customer access to low level network traffic is impossible, it must rely on Providers for IDS/IPS, monitoring and alerting."[128]

---

127 Anoosh Saboori & Brad Jones, *Snowflake Strengthens Security with Default Multi-Factor Authentication and Stronger Password Policies*, Snowflake (Sept. 13, 2024), https://www.snowflake.com/en/blog/multi-factor-identification-default/.

128 *PCI SSC Cloud Computing Guidelines*, *supra n.* 64, at 63.

274. Snowflake, through these data security failings, was negligent and breached its duty to Plaintiffs and Class Members to protect their Personal Information—information which it knew was sensitive—stored on Snowflake's Data Cloud.

275. Snowflake's breach of its duty proximately caused the Data Breach. Had Snowflake maintained adequate data security practices (such as requiring or allowing customers to require MFA, credential rotation, or intrusion detection), the Data Breach would have been prevented.

276. Snowflake's data security failings also constitute an unfair trade practice because of its failure to maintain reasonable and appropriate data security.

277. Rather than take responsibility for its actions, Snowflake foisted the blame and responsibility onto the Spoke Defendants to "query for unusual activity and conduct further analysis to prevent unauthorized user access."[129]

278. Even after the Data Breach, Snowflake insists that it was not breached. Despite failing to implement many basic cybersecurity measures, which could have prevented the Data Breach, and despite adopted a "shared responsibility" model, Snowflake insisted that it was not responsible. Snowflake's CEO Sridhar

[129] Alert, *Snowflake Recommends Customers Take Steps to Prevent Unauthorized Access*, CISA (June 3, 2024), https://www.cisa.gov/news-events/alerts/2024/06/03/snowflake-recommends-customers-take-steps-prevent-unauthorized-access.

Ramaswamy's representation to its investors was, "[a]s extensively reported, the issue wasn't on the Snowflake side. . . . After multiple investigations by internal and external cybersecurity experts, we found no evidence that our platform was breached or compromised."[130]

279. Snowflake refuses to take responsibility for its failure to implement basic cybersecurity policies and protocols which would have prevented the Data Breach, even though it has implemented several of those policies since the breach occurred.

280. But the details set forth in the Mandiant Report are not the only cybersecurity failings of Snowflake. The threat actor was also able to sign in through Snowflake's ServiceNow account using stolen Snowflake credentials, bypassing Snowflake's identity and access management platform, which provided single sign-on capabilities for Snowflake.[131]

281. It was reported that the threat actor was able to exfiltrate massive amounts of data from Snowflake corresponding to hundreds of companies.[132]

---

130 Matt Kapko, *After a wave of attacks, Snowflake insists security burden rests with customers*, CybersecurityDive (Aug. 22, 2024), https://www.cybersecuritydive.com/news/snowflake-security-responsibility-customers/724994/.

131 Hudson Rock Report, *supra* n. 24.

132 *Id.* According to Hudson Rock, the threat actor used a Snowflake employee's work credentials using info-stealing malware to exfiltrate data from Snowflake's customer cloud accounts.

282. Hudson Rock first reported the intrusion by the threat actor into Snowflake's systems; however, after receiving legal pressure from Snowflake, it removed its online report.[133]

IV. Snowflake's actions injured Plaintiffs and Class Members.

283. Snowflake's breach of its duty of care and engagement in unfair trade practices caused injury to Plaintiff and Class Members, as discussed herein.

284. Snowflake is liable for the injuries suffered by each Plaintiff and Class Member by virtue of its role as a data storage provider that stored, and failed to protect, the data of all the Spoke Defendants.

285. To avoid duplication and for organizational purposes, this section incorporates by reference the following sections that allege in detail the injuries suffered by Plaintiffs and Class Members: Part One, Section III; Part Three, Section VI; Part Four, Section V; Part Five, Section V; and Part Six, Section IV.

V. Class action allegations as to Snowflake.

286. Plaintiffs bring this action on their own behalf, and on behalf of the following Class and Subclasses (referred to collectively as the "Snowflake Classes"):

---

[133] Jessica Lyons, *Hudson Rock yanks report fingering Snowflake employee creds snafu for mega-leak*, The Register (Jun 4, 2024), https://www.theregister.com/2024/06/04/snowflake_report_pulled/.

- **Nationwide Snowflake Class.** All individuals residing in the United States whose Personal Information was identified as compromised in the Data Breach by a Spoke Defendant.
- **State-Specific Subclasses.** As described in this Section below, all individuals residing in a specific state whose Personal Information was identified as compromised in the Data Breach by a Spoke Defendant.
- **California CCPA Snowflake Subclass.** All individuals residing in California whose nonencrypted and nonredacted personal information, as defined in Cal. Civ. Code § 1798.150(a), was identified as compromised in the Data Breach by a Spoke Defendant.

287. Plaintiffs' proposed class definitions against Snowflake are inclusive of proposed national and state class definitions against the Spoke Defendants.

288. Excluded from the Snowflake Classes are Snowflake's officers and directors, any entity in which Snowflake has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Snowflake. Excluded also from the Snowflake Classes are members of the judiciary to whom this case is assigned, their families and members of their staff.

289. Plaintiffs reserve the right to amend or modify the definition of the Snowflake Classes or create additional subclasses as this case progresses.

290. **Numerosity.** The members of the Snowflake Classes are so numerous that joinder of all of them is impracticable. Public reporting presently indicates that there are hundreds of millions of individuals whose Personal Information was stored on Snowflake's Data Cloud and exfiltrated in the Data Breach.

291. **Commonality.** There are questions of fact and law common to the Snowflake Classes, which predominate over individualized questions. These common questions of law and fact include, but are not limited to:

- Whether Snowflake had a duty to protect the Personal Information of Plaintiffs and Snowflake Class Members, and whether it breached that duty.
- Whether Snowflake knew or should have known that its data security practices were deficient.
- Whether Snowflake's data security systems were consistent with industry standards prior to the Data Breach.
- Whether Snowflake's failure to require customers to implement MFA, employ credential rotation, and employ other industry standard data security measures violated a standard of care or laws.
- Whether Plaintiffs and Snowflake Class members are entitled to actual damages, punitive damages, treble damages, statutory damages, nominal damages, general damages, and/or injunctive relief.

292. **Typicality.** Plaintiffs' claims are typical of those of other Snowflake Class members because the Plaintiffs' Personal Information, like that of every other Snowflake Class Member, was compromised in the Data Breach

293. **Adequacy of Representation.** Plaintiffs will fairly and adequately represent and protect the interest of the Snowflake Class members. Plaintiffs' Counsel are competent and experienced in litigating class actions.

294. **Predominance.** Snowflake engaged in a common course of conduct toward the Plaintiffs and Snowflake Class members, in that their data was stored on

the same Snowflake Data Cloud network and unlawfully accessed in the same manner. The common issues arising from Snowflake's conduct affecting Class Members listed above predominate over any individualized issues. Adjudication of these common issues in a single action will advance judicial economy.

295. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of the claims of the Snowflake Classes. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Snowflake Class members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Snowflake Class members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Snowflake. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Snowflake Class Member.

296. **Injunctive Relief.** Snowflake has acted on grounds that apply generally to the Snowflake Classes as a whole such that class certification, injunctive relief, and declaratory relief are appropriate on a class-wide basis.

297. **Issue Certification.** Likewise, certain issues are appropriate for certification because such claims present common issues whose resolution would advance the disposition of this matter. Such issues include, but are not limited to:

- Whether Snowflake owed a legal duty to Plaintiffs and Snowflake Class members to protect their Personal Information.
- Whether Snowflake's data security measures were inadequate in light of applicable regulations and industry standards.
- Whether Snowflake's data security measures were negligent or reckless.

298. **Identification of Class Members via Objective Criteria.** Finally, all members of the proposed Snowflake Classes are readily identifiable using objective criteria. Both Snowflake and the Spoke Defendants have access to the names and contact information of Snowflake Class members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by the Spoke Defendants.

VI. Causes of action as to Snowflake.

FIRST CLAIM FOR RELIEF
Negligence
On behalf of All Plaintiffs and the Nationwide Snowflake Class

299. Plaintiffs repeat and re-allege the allegations contained in Paragraphs 1 through 150, as well as Part One and Part Two, as set forth fully herein.

300. Snowflake owed a duty under common law to Plaintiffs and Nationwide Snowflake Class Members to exercise reasonable care in obtaining,

retaining, securing, safeguarding, and deleting their Personal Information in its possession from being compromised, stolen, or misused by unauthorized persons.

301. Specifically, this duty included, among other things: (a) implementing industry standard data security safeguards to protect the Personal Information of Plaintiffs and Nationwide Snowflake Class members relating to MFA, rotating credentials, and restricting access privileges; (b) maintaining, testing, and monitoring Snowflake's security systems to ensure that Personal Information was adequately secured and protected; and (c) implementing intrusion detection systems and notifying customers of suspicious intrusions.

302. Snowflake's duty to use reasonable care arose from several sources, as described herein, including that Snowflake knew or should have known that the information it stored for the Spoke Defendants was sensitive, and that failing to take adequate steps to secure and protect the data would foreseeably lead to a Data Breach which could injure individual consumers.

303. Snowflake had a common law duty to prevent foreseeable harm to others. This duty existed because Snowflake stored valuable Personal Information that is routinely targeted by cyber criminals. Plaintiffs and Nationwide Snowflake Class members were the foreseeable and probably victims of any compromise to inadequate data security practices maintained by Snowflake.

304. Snowflake further assumed a duty of reasonable care in making representations in marketing materials that their data storage services were secure and offered "built-in" and turnkey solutions for data security compliance.

305. Snowflake breached its duty owed to the Plaintiffs and Nationwide Snowflake Class members by failing to maintain adequate data security practices that conformed with industry standards, and were therefore negligent.

306. But for Snowflake's negligence, the Personal Information of the Plaintiffs and Nationwide Snowflake Class members would not have been stolen by cybercriminals in the Data Breach.

307. As a direct and proximate result of Snowflake's breach of its duties, Plaintiffs and Nationwide Snowflake Class members have suffered injuries as detailed herein.

308. As a direct and proximate result of Snowflake's negligence, Plaintiffs and Nationwide Snowflake Class members are entitled to damages, including compensatory, punitive, nominal damages, and/or general damages in an amount to be proven at trial.

SECOND CLAIM FOR RELIEF
Violation of the Montana Unfair Trade Practices & Consumer Protection Act (Mont. Code Ann. § 30-14-101, *et seq.*) ("MUTPCPA")

On behalf of All Plaintiffs and the Nationwide Snowflake Class
In the alternative, on behalf of Plaintiffs Madden and Murphy and a Snowflake Subclass of Montana Residents

309. Plaintiffs repeat and re-allege the allegations contained in Paragraphs 1 through 150, as well as Part One and Part Two, as set forth fully herein.

310. Plaintiffs and Nationwide Snowflake Class members are "consumers" under the MUTPCPA because they purchased ticketing services for personal, family, or household purposes. Mont. Code Ann. § 30-14-102(1).

311. Snowflake is a "person[]" under the MUTPCPA, which is defined to mean "natural persons, corporations, trusts, partnerships, incorporated or unincorporated associations, and any other legal entity." Mont. Code Ann. § 30-14-102(6).

312. Snowflake engaged in "trade" and "commerce" as defined by the MUTPCPA because it operates its data cloud services and makes decisions regarding data security from its Montana headquarters. Mont. Code Ann. § 30-14-102(8)(a) (defining "trade" and "commerce" to mean the "sale, or distribution of any services . . . tangible or intangible . . . wherever located, and includes any trade or commerce directly or indirectly affecting the people of this state"). The State of Montana has a compelling interest in ensuring that companies within its jurisdiction follow its laws.

313. Snowflake engaged in unfair trade practices prohibited by the MUTPCPA. Mont. Code Ann. § 30-14-103.

314. Snowflake engaged in unfair trade practices when it failed to maintain reasonable data security practices to safeguard the Personal Information of Plaintiffs and Snowflake Class members, as described herein.

315. Snowflake's conduct offends established public policy and is immoral, unethical, oppressive, unscrupulous and substantially injurious to consumers.

316. Montana has the most significant relationship with Snowflake's unfair trade practices alleged herein such that it is proper to apply the MUTPCPA to the Nationwide Snowflake Class. Snowflake is headquartered in Montana. As Snowflake made decisions regarding the data security policies and practices that are challenged in this action from its Montana headquarters, the conduct causing Plaintiffs' and Class members' injury occurred in Montana. Finally, Montana has a strong interest in regulating the trade practices of companies headquartered within its borders.

317. Plaintiffs and Snowflake Class members have suffered injury as a result of Snowflake's unfair trade practices, as described herein.

318. As a direct and proximate result of Snowflake's unfair trade practices, Plaintiffs and Snowflake Class members are entitled to injunctive relief, damages, including actual damages in an amount to be proven at trial or statutory damages of $500, whichever is greater, treble damages of actual damages, and reasonable attorneys' fees. Mont. Code Ann. § 30-14-133.

THIRD CLAIM FOR RELIEF
Violation of California Consumer Privacy Act
("CCPA") (Cal. Civ. Code § 1798.100), *as amended*
On behalf of Plaintiffs Swain and Xian
and the California CCPA Snowflake Subclass

319. Plaintiff Swain and Xian (collectively, the "California Plaintiffs") repeat and re-allege the allegations contained in Paragraphs 1 through 150, as well as Part One and Part Two, as set forth fully herein.

320. Cal. Civ. Code § 1798.150(a) of the CCPA provides that "[a]ny consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5 . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action" for statutory damages, actual damages, injunctive relief, declaratory relief and any other relief the court deems proper.

321. Snowflake violated California Civil Code § 1798.150 of the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the Personal Information of the California Plaintiffs and the Snowflake California Subclass Members. Snowflake's actions were reckless. As a direct and proximate result of these security

failures, California Plaintiffs and Snowflake California Subclass Members' Personal Information was subject to unauthorized access and exfiltration, theft, or disclosure.

322. Snowflake is a "business" under the meaning of Cal. Civil Code § 1798.140 because it is a "corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners" that "collects consumers' personal information" and is active "in the State of California" and "had annual gross revenues in excess of twenty-five million dollars ($25,000,000) in the preceding calendar year." Cal. Civil Code § 1798.140(d).

323. California Plaintiffs and Snowflake California Subclass Members are "consumers" as defined by Cal. Civ. Code § 1798.140(g) because they are natural persons who reside in California.

324. California Plaintiffs and Snowflake California Subclass Members seek injunctive or other equitable relief to ensure Snowflake hereinafter adequately safeguard their Personal Information by implementing reasonable security procedures and practices. Such relief is particularly important because Snowflake continues to hold Personal Information, including that of California Plaintiffs and Snowflake California Subclass Members.

325. California Plaintiffs and Snowflake California Subclass Members have an interest in ensuring that their Personal Information is reasonably protected, and Snowflake has demonstrated a pattern of failing to adequately safeguard this information.

326. Notice related to Plaintiffs' intention to bring claims pursuant to the CCPA was sent to Snowflake on December 27, 2024, and also provided previously by other plaintiffs and their counsel. Despite receipt of the letter, Snowflake has refused to cure its violations as demanded by Plaintiffs.

327. Snowflake failed to take sufficient and reasonable measures to safeguard its data security systems and protect California Plaintiffs and Snowflake California Subclass Members' Personal Information from unauthorized access. Snowflake's failure to maintain adequate data protections subjected California Plaintiffs and Snowflake California Subclass Members' Personal Information to exfiltration and disclosure by malevolent actors.

328. The unauthorized access, exfiltration, theft, and disclosure of California Plaintiffs and Snowflake California Subclass Members' Personal Information was a result of Snowflake's violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Personal Information.

329. Snowflake's unreasonable security practices include, but are not limited to: (a) failing to implement industry standard data security safeguards to protect the Personal Information of California Plaintiffs and Class Members relating to MFA, rotating credentials, and restricting access privileges; (b) failing to maintain, test, and monitor Snowflake security systems to ensure that Personal Information was adequately secured and protected; (c) failing to implement intrusion detection systems and notifying customers of suspicious intrusions.

330. California Plaintiffs and Snowflake California Subclass Members have suffered actual injury as detailed herein, and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

331. Snowflake's violations of Cal. Civ. Code § 1798.150(a) are a direct and proximate cause of the Data Breach.

332. California Plaintiffs and Snowflake California Subclass Members seek all monetary and non-monetary relief allowed by law, including actual, general, or nominal damages; declaratory and injunctive relief, including an injunction barring Snowflake from disclosing their Personal Information without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper.

333. California Plaintiffs and Snowflake California Subclass Members are further entitled to the greater of statutory damages in an amount not less than one

hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater. See Cal. Civ. Code § 1798.150(b).

334. As a result of Snowflake's failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, California Plaintiffs and Snowflake California Subclass Members seek actual damages, statutory damages, injunctive relief (including public injunctive relief), and declaratory relief, and any other relief as deemed appropriate by the Court.

FOURTH CLAIM FOR RELIEF
Violation of Massachusetts General Law Chapter 93A
("MGL Chapter 93A")
On behalf of Plaintiff O'Hara and a Snowflake Subclass of Massachusetts Residents

335. Plaintiff O'Hara repeats and re-alleges the allegations contained in Paragraphs 1 through 150, as well as Part One and Part Two, as set forth fully herein.

336. Plaintiff O'Hara and Massachusetts Snowflake Subclass Members are "persons" under MGL Chapter 93A because they are natural persons. Mass. Gen. L. Ch 93A § 1(a).

337. Snowflake is a "person[]" under MGL Chapter 93A because it is a corporation. Mass. Gen. L. Ch 93A § 1(a).

338. Snowflake engaged in "trade" and "commerce" as defined by MGL Chapter 93A because in the course of selling its data cloud services, it hosts the Personal Information of Massachusetts residents on its Data Cloud, including Plaintiff O'Hara and Massachusetts Snowflake Subclass Members. Mass. Gen. L. Ch. 93A § 1(b).

339. Snowflake engaged in unfair trade practices prohibited by MGL Chapter 93A. Mass. Gen. L. Ch. 93A § 2(a), and regulations promulgated thereunder, including but not limited to 201 CMR 17.00.

340. Snowflake engaged in unfair trade practices when it failed to maintain reasonable data security practices to safeguard the Personal Information of Plaintiff O'Hara and Massachusetts Snowflake Subclass Members, including: (a) failing to implement industry standard data security safeguards to protect the Personal Information of Plaintiff O'Hara and Massachusetts Snowflake Subclass Members relating to MFA, rotating credentials, and restricting access privileges; (b) failing to maintain, test, and monitor Snowflake's security systems to ensure that Personal Information was adequately secured and protected; and (c) failing to implement intrusion detection systems and notifying customers of suspicious intrusions.

341. Snowflake's conduct offends established public policy and is immoral, unethical, oppressive, unscrupulous and substantially injurious to consumers.

342. Plaintiffs and Snowflake Class members have suffered injury as a result of Snowflake's unfair trade practices, as described herein.

343. Notice related to Plaintiff O'Hara and the Massachusetts Snowflake Subclass Members' intention to bring claims pursuant to the MGL was sent to Snowflake on December 27, 2024. Despite receipt of the letter, Snowflake has refused to cure its violations as demanded by Plaintiff O'Hara and the Massachusetts Snowflake Subclass' Members.

344. As a direct and proximate result of Snowflake's unfair trade practices, Plaintiff O'Hara and Massachusetts Snowflake Subclass Members are entitled to injunctive relief, damages, including actual damages in an amount to be proven at trial or statutory damages of $25, whichever is greater, treble damages of actual damages, and reasonable attorneys' fees. Mass. Gen. L. Ch. 93A § 9(3).

FIFTH CLAIM FOR RELIEF
Violation of District of Columbia Consumer Protection Procedures Act, D.C. Code § 28-3901, *et seq.* ("D.C. CPPA")
(On behalf of Plaintiffs D. Thomas and Lively and a Snowflake Subclass of District of Columbia Residents)

345. Plaintiffs D. Thomas and Lively (the "Washington D.C. Plaintiffs") repeat and re-allege the allegations contained in Paragraphs 1 through 150, as well as Part One and Part Two, as set forth fully herein.

346. A violation of the Washington D.C. Security Breach Protection Amendment Act of 2020 ("D.C. SBPAA"), including D.C. Code § 28-3852,

constitutes a per se unfair or deceptive trade practice under the D.C. CPPA. *See* D.C. Code § 28-3853; D.C. Code § 28-3904 (kk).

347. D.C. Code § 28-3852.01 of the D.C. SBPAA provides: "To protect personal information from unauthorized access, use, modification, disclosure, or a reasonably anticipated hazard or threat, a person or entity that owns, licenses, maintains, handles, or otherwise possesses personal information of an individual residing in the District shall implement and maintain reasonable security safeguards, including procedures and practices that are appropriate to the nature of the personal information and the nature and size of the entity or operation."

348. Snowflake violated the D.C. SBPAA, and therefore the D.C. CPPA, by failing to implement and maintain reasonable security safeguards, including procedures and practices appropriate to the nature of the personal information and the nature and size of Snowflake's operations. Among other things, Snowflake failed to maintain reasonable data security practices to safeguard the Personal Information of the Washington D.C. Plaintiffs and D.C. Snowflake Subclass Members, including: (a) failing to implement industry standard data security safeguards to protect the Personal Information of the Washington D.C. Plaintiffs and Washington D.C. Snowflake Subclass Members relating to MFA, rotating credentials, and restricting access privileges; (b) failing to maintain, test, and monitor Snowflake's security systems to ensure that Personal Information was

adequately secured and protected; and (c) failing to implement intrusion detection systems and notifying customers of suspicious intrusions.

349. Snowflake's actions were reckless. As a direct and proximate result of its security failures, Washington D.C. Plaintiffs and Washington D.C. Subclass Members' Personal Information was subject to unauthorized access and exfiltration, theft, and/or disclosure.

350. In addition to its per se violation of the CPPA, Snowflake engaged in unfair trade practices prohibited by the D.C. CPPA. D.C. Code § 28-3904.

351. The Washington D.C. Plaintiffs and Washington D.C. Snowflake Subclass Members are "consumers" under the D.C. CPPA because they "receive[d] consumer services" or "otherwise provide[d] the economic demand for a trade practice." D.C. Code § 28-3901(a)(2).

352. Snowflake is a "merchant" under the D.C. CPPA because it "suppl[ies] the goods or services which are . . . the subject of a trade practice." D.C. Code § 28-3901(a)(3).

353. Snowflake's cloud data storage services provided to the Spoke Defendants are "trade practices" because they are acts that "directly or indirectly . . . effectuate, a sale, lease or transfer, of consumer goods or services." D.C. Code § 28-3901(a)(6).

354. Snowflake's conduct offends established public policy and is immoral, unethical, oppressive, unscrupulous and substantially injurious to consumers. The harm done sufficiently outweighs any justifications or motives for Snowflake's practice of collecting and storing Personal Information without appropriate and reasonable safeguards to protect such information in place. Consumers could not have reasonably avoided the harm inflicted by Snowflake.

355. As a result of Snowflake's violations of the D.C. CPPA, Washington D.C. Plaintiffs and D.C. Subclass members have suffered and will suffer injury, as described above.

356. As a direct and proximate result of Snowflake's unlawful and unfair trade practices, Washington D.C. Plaintiffs and D.C. Subclass Members are entitled to injunctive relief, damages, including actual damages in an amount to be proven at trial or statutory damages of $1,500, whichever is greater, treble damages of actual damages, and reasonable attorneys' fees. D.C. Code § 28-3905(k)(1)(A), (k)(2).

SIXTH CLAIM FOR RELIEF
Invasion of Privacy (Public Disclosure of Private Facts)
On behalf of the AT&T Plaintiffs, the Nationwide AT&T Class, the Nationwide Cricket Wireless Class, and the Nationwide Non-Customer AT&T Class (defined infra)

357. The AT&T Plaintiffs ("Plaintiffs" for purposes of this Claim) repeat and re-allege the allegations contained in Paragraphs 1 through 150, as well as Part One, Part Two, and Part Six, as set forth fully herein.

358. The Plaintiffs' Personal Information described in Part One, Section III, and Part Six, Section III-IV, are of a private, secluded, and highly personal nature, the disclosure of which would be highly offensive to a reasonable person and is not a matter of legitimate public concern.

359. Snowflake, in failing to implement reasonable cyber security policies and practices, disclosed Plaintiffs' Personal Information to cybercriminals and nefarious third parties, who in turn further disclosed Plaintiffs' Personal Information on the dark web by advertising and selling the stolen Personal Information. These disclosures gave publicity to Plaintiffs' Personal Information.

360. Snowflake had no legitimate basis to disclose Plaintiffs' Personal Information to cybercriminals or nefarious third parties.

361. It was entirely foreseeable that this information would be disclosed to nefarious third parties if reasonable cybersecurity measures were not taken. The failure to implement MFA, along with the other cybersecurity failings as described herein, has resulted in data breaches in the past, and not implementing reasonable cybersecurity measures meant that it was foreseeable that highly personal and sensitive information would be exposed in a data breach.

362. Snowflake was reckless in failing to implement reasonable cybersecurity measures.

363. Plaintiffs have suffered injury as a result of Snowflake's public disclosure of their private facts, as described herein.

364. Plaintiffs seek all monetary and non-monetary relief allowed by law, including actual, nominal, or general damages; declaratory and injunctive relief, including an injunction barring Snowflake from disclosing their Personal Information without their consent; and any other relief that is just and proper.

PART THREE: TICKETMASTER AND LIVE NATION

366. Plaintiffs Eric Anderson, Charles Fitzgerald, Susie Garcia, Valerie Lozoya, LaVonne Madden, Jolinda Murphy, Lauren Neve, Molly O'Hara, Dekima Thomas, and Christina Xian (collectively, the "Ticketmaster Plaintiffs") are named in this Representative Complaint to pursue claims against Ticketmaster.[134]

I. Ticketmaster's business and data security promises.

367. Consumers are largely unable to purchase concert tickets or enjoy concerts without working through Live Nation, and its wholly owned subsidiary Ticketmaster.

368. Live Nation and Ticketmaster control approximately 70% of the American market for live event ticketing, selling hundreds of millions of tickets per year.[135] Live Nation reported a quarterly revenue of $7.7 billion in November 2024.[136]

---

134 Ticketmaster and Live Nation are collectively referred to herein, except as expressly delineated, as "Ticketmaster" or the "Ticketmaster Defendants."

135 Daniel Allen, *Does Live Nation Own Ticketmaster? The Complete Story Behind Entertainment's Biggest Merger*, The Ticket Lover (Oct. 28, 2024), https://theticketlover.com/does-live-nation-own-ticketmaster/).

136 Live Nation, *LIVE NATION ENTERTAINMENT REPORTS THIRD QUARTER 2024 RESULTS* (Nov. 11, 2024), https://www.livenationentertainment.com/2024/11/live-nation-entertainment-reports-third-quarter-2024-results/.

369. Live Nation considers itself the world's leading live entertainment ticketing sales and marketing company based on the number of tickets sold. In 2023, Ticketmaster distributed over 620 million tickets through www.ticketmaster.com, www.livenation.com, the companies' mobile apps, and other websites and retail outlets. The same year, Live Nation connected over 765 million individuals to live events.[137]

370. Live Nation and Ticketmaster are highly integrated with respect to collecting customer Personal Information, sharing customer Personal Information, and developing and implementing privacy policies. To provide several examples, near the time of the Data Breach:

- When a consumer purchases tickets through Live Nation, they are often informed the purchase is "powered by Ticketmaster" or redirected to a Ticketmaster purchasing portal.
- Live Nation and Ticketmaster maintain similar privacy policies that list the following identical Live Nation point of contact for consumers with privacy inquiries: Attention: Privacy Officer, Legal, Live Nation Entertainment, Inc., 9348 Civic Center Drive, Beverly Hills, CA 90210.[138]

---

[137] Live Nation, 2024 Annual Report (Form 10-K) at 2 (Feb. 22, 2024), https://investors.livenationentertainment.com/sec-filings/annual-reports/content/0001335258-24-000017/0001335258-24-000017.pdf.

[138] *Compare* Live Nation Entertainment, *Privacy Policy* ("Live Nation, *Privacy Policy*"), https://web.archive.org/web/20240222185813/https://help.livenation.com/hc/en-us/articles/10464047306641-Live-Nation-Entertainment-Privacy-Policy (archived Feb. 22, 2024), *with* Ticketmaster, *PRIVACY POLICY* ("Ticketmaster, *Privacy*

- Live Nation's Privacy Policy discloses: "We will share information within the Live Nation family of companies. This may include Ticketmaster and Live Nation-owned or operated venues, for example."[139]

- Ticketmaster's Privacy Policy likewise discloses that customer data will be shared "[w]ithin the Ticketmaster group" and directs consumers to write to Live Nation's corporate address with privacy inquiries.[140]

371. Ticketmaster requires consumers who purchase tickets on their platform to provide their Personal Information to Ticketmaster, both to facilitate the ticket sales and for Ticketmaster's own business purposes. Ticketmaster promises to keep consumers' Personal Information secure and does not allow consumers to opt out of sharing their Personal Information.

372. Ticketmaster made express commitments to protecting consumer Personal Information in its Privacy Policy, assuring consumers in a caption titled, *Looking After Your Information*, "We have security measures in place to protect your information."[141]

Policy"), *Contact Us*, https://web.archive.org/web/20240226041015/https://privacy.ticketmaster.com/privacy-policy#contact-us (archived Feb. 26, 2024).

139 Live Nation, *Privacy Policy*, *supra* n. 138.

140 Ticketmaster, *Privacy Policy*, *supra* n. 138.

141 Ticketmaster, *Privacy Policy*, *supra* n. 138.

373. Ticketmaster publicly represented that data security forms a crucial aspect of its business model. For instance, on a segment of Ticketmaster LLC's website, the company stated:

> "Our goal is to maintain your trust and confidence by handling your personal information with respect and putting you in control."[142]
>
> "As a global company, our fans are located all over the world, depending on your market there are specific laws and regulations around privacy rights such as the GDPR in Europe, LGPD in Brazil and CCPA in United States."[143]
>
> "We have security measures in place to protect your information."[144]

374. Live Nation also maintained a privacy policy section, affirming its adherence to various state and federal laws.[145]

375. Ticketmaster's Privacy Policy includes specific commitments relating to "Data Transfers," which provides as follows[146]:

> When transferring information, there are strict rules in place to ensure your data is still protected to the highest standard. Where we do this, we will ensure that appropriate safeguards are put in place. Where your information is transferred outside of your local market, we use contractual measures and internal mechanisms requiring the recipient to comply with the privacy standards of the exporter[.]

---

142 Ticketmaster, *Privacy* Policy, *supra* n. 138.

143 Ticketmaster, *Privacy* Policy, *supra* n. 138.

144 *Id.*

145 Live Nation, *Privacy* Policy, *supra* n. 138.

146 *Id.*

376. Ticketmaster maintains a website captioned, *Our Commitments*, which make the following representations concerning privacy (the "Privacy Commitments")[147]:

- **Fair & Lawful**. We comply with all applicable data protection laws and listen to your expectations when it comes to how your information is handled.
- **Security & Confidentiality.** The security of our fans' information is a priority for us. We take all necessary security measures to protect personal information that's shared and stored with us.
- **Third Parties & Partners.** We work with our partners to put on amazing live events and provide additional services that we think you'll love. We always ask them to maintain the same standards of privacy.
- **Privacy By Design.** We embed privacy in the development of our products and services to ensure that we always respect your personal information.
- **Storage & Retention**. We store and use your data only as long as we need to, from complying with our legal obligations to making sure you know when your favorite artist is on tour.

377. Ticketmaster represented on a separate FAQ website that it complies with the PCI DSS and that it "take[s] compliance very seriously."[148]

---

147 Ticketmaster, *Our Commitments*, https://web.archive.org/web/20230517182539/https://privacy.ticketmaster.com/our-commitments (archived May 17, 2023) ("Privacy Commitments").

148 Ticketmaster Business, *Define the Future of Live with Us*, https://web.archive.org/web/20240319080146/https://business.ticketmaster.com/web/20240319080146/https://business.ticketmaster.com/web/20240319080146/https://business.ticketmaster.com/ (archived Mar. 19, 2024).

378. Ticketmaster relies on multiple third-party service providers to carry out key business functions including payment processing, marketing, customer service, and data storage.[149]

379. At the same time, Ticketmaster states that it is "committed to being the safest, most reliable ticket marketplace in the world."[150] Ticketmaster recommended to consumers that they could take several steps to secure their online accounts:

- "Make sure you're using a strong password for your account. Your password should be unique to your Ticketmaster account, and therefore not used for any other accounts (banking, retail sites, email, etc). You can easily reset your password if you need to."[151]
- "Another good way to protect your tickets is to make sure the phone number associated with your Ticketmaster account is up to date. For extra security during a ticket purchase, you may also be asked to authenticate your account by inputting a code sent to your phone number."[152]
- "Just like you want to make sure your Ticketmaster password is unique, you should do the same for your personal email. Make

---

149 Ticketmaster, *Privacy Policy: Who We Share Your Data With & Why*, https://web.archive.org/web/20240219050226/https://privacy.ticketmaster.com/privacy-policy#who-we-share-your-data-with-&-why (archived Feb. 19, 2024).

150 Ticketmaster, *How to Secure Your Account and Protect Your Tickets* (Apr. 12, 2024), https://web.archive.org/web/20240426053554/https://blog.ticketmaster.com/account-security-tips-password-protect-tickets/.

151 *Id.*

152 *Id.* In other words, Ticketmaster suggested to consumers that they could keep their account safe by enabling MFA.

> sure you're using a strong, unique password there, too. If your email gets hacked, which unfortunately does happen, it could allow bad actors to use it to try to gain access to your Ticketmaster account."[153]
>
> - But be aware of scammers sharing fake information about Ticketmaster, including fake customer service phone numbers that appear in search engines.[154]

380. While Ticketmaster told consumers that *they* should take multiple steps to keep their Personal Information secure, because Ticketmaster used third-party service providers to maintain Personal Information (and to employ the same data privacy standards as those employed by Ticketmaster),[155] Ticketmaster's customers actually had no way to keep their information safe—even following the steps above—if Ticketmaster and its service providers were not taking the most basic steps to secure consumer information.

381. Ticketmaster is a Snowflake customer. Ticketmaster stores the Personal Information of its consumers on Snowflake's Data Cloud services, which include customers' names, addresses, contact information (email and phone numbers), and payment card information.

---

153 *Id.*

154 *Id.* In other words, Ticketmaster warned consumers that they could fall prey to phishing schemes.

155 Ticketmaster, *Our Commitments*, *supra* n. 147.

382. Ticketmaster did not employ rudimentary security measures that were available to it through Snowflake, including implementing a policy mandating that its users employ MFA on their accounts.

II. Ticketmaster employs its significant market power to deprive consumers of meaningful choice.

383. Because Ticketmaster and Live Nation control a significant portion of the market, consumers have no choice but to use their services to buy live music tickets.

384. Accordingly, consumers have no choice about which company to provide their Personal Information to, nor do they have any ability to negotiate the terms and conditions which govern their relationship with Ticketmaster.

385. Without actual competition in the marketplace, consumers are left with "take-it-or-leave-it" policies concerning data protection and even dispute resolution.

386. Ticketmaster's terms and conditions contain a number of unfair provisions related to dispute resolution.

387. First, Ticketmaster's customer agreements provided that it could change terms and conditions online, with changes taking effect immediately upon posting when the customer next visits the website without adequate notice.

388. Second, Ticketmaster's customer agreement was changed to provide that a term concerning dispute resolution applied retroactively to past disputes.

389. Third, Ticketmaster's terms are excessively one-sided, allowing exceptions for litigation on intellectual property disputes and limits on liability and indemnity clauses—provisions which only benefitted Ticketmaster. Beyond that, Ticketmaster's terms provided the ability to appeal decisions by an arbitrator in court only in ways that benefitted Ticketmaster.

390. Fourth, although Ticketmaster's prior arbitration agreement ("JAMS agreement") designates JAMS, an established arbitration forum, as the dispute resolution forum, the new agreement ("New Era agreement"), which is Section 17 of Ticketmaster's Terms of Use, designates New Era ADR as the dispute resolution forum.[156] New Era ADR was launched in April 2021 with the mission of "helping businesses settle legal disputes" by creating rules that "make[] sense for businesses" and that also benefit "law firms, who are able to provide an improved client experience" to businesses "and handle a higher volume of cases" that are filed by consumers.[157] New Era ADR advertises having launched "with around 10 clients," i.e., businesses, who have designated New Era ADR as the forum "in nearly 700 contracts," which New Era ADR expected "will provide a pipeline of potential

---

156 Ticketmaster, *Terms of Use*, https://help.ticketmaster.com/hc/en-us/articles/10468830739345-Terms-of-Use (last updated July 2, 2021).

157 Jim Dallke, *This startup is helping businesses settle legal disputes completely online*, Chicago Inno (May 3, 2021), https://www.bizjournals.com/chicago/inno/stories/profiles/2021/05/03/onlinearbitration-mediation-startup-new-era-adr.html (last accessed November 1, 2024).

clients," i.e., additional businesses, "down the road."[158] New Era ADR adopted unconscionable and unenforceable rules concerning the ability to participate in arbitration, such as lack of or limited discovery, procedural limitations, the one-sided selection of arbitrators, and a limited right to appeal.

391. Ticketmaster's market power prevented consumers from making a meaningful choice in purchasing concert tickets, providing Personal Information to companies, or engaging in dispute-resolution procedures.

III. Ticketmaster owed a duty of care to Plaintiffs and Class Members.

392. Because Ticketmaster deprived Plaintiffs of meaningful choice in the selection of a ticket provider, then at the very least it could have protected Personal Information to ensure that the data was not misused. Instead, Ticketmaster did not even employ the bare minimum of security measures on its Snowflake accounts.

393. As a condition of purchasing a ticket from Ticketmaster, consumers, including the Ticketmaster Plaintiffs, provide their Personal Information to Ticketmaster, including their names, contact information, and payment card information such as credit card number and expiration date.

394. Ticketmaster, in collecting such sensitive Personal Information from consumers, owed a duty of care to consumers, including the Ticketmaster Plaintiffs,

158 *Id*.

to exercise reasonable care in maintaining, protecting, and securing their Personal Information.

395. Ticketmaster, by mandating the receipt of sensitive Personal Information from consumers as a condition of purchase, implied its assent to consumers to protect their Personal Information. Consumers expected Ticketmaster to protect their Personal Information when they provided it as a condition of purchase.

396. Ticketmaster owed a common law duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Personal Information in Snowflake's possession from being compromised, accessed, stolen, or misused by unauthorized parties.

397. Ticketmaster owed a common law duty to Plaintiffs and Class Members to supervise Snowflake in the collection, storage, and security of Plaintiffs' and Class Members' Personal Information.

398. Ticketmaster's duty of reasonable care is established by governmental regulations and industry guidance establishing industry standards for data security to safeguard Personal Information stored on cloud platforms, as described herein.

399. Ticketmaster owed a statutorily imposed duty to Plaintiffs and Class Members to refrain from unfair and deceptive practices.

400. Ticketmaster and Live Nation understood that they owed a duty of care to Plaintiffs and Class Members to keep their information safe and secure; they acknowledged that data breaches could cause substantial harm to individuals, and were foreseeable. This duty extended to Ticketmaster's oversight of any third-parties or vendors in which it entrusted its customers' Personal Information. On February 22, 2024, Live Nation, in its SEC Annual Report, explicitly identified data security as a risk facing the business, and stated as follows[159]:

> Due to the nature of our business, we process, store, use, transfer and disclose certain personal or sensitive information about our customers and employees. Penetration of our network or other misappropriation or misuse of personal or sensitive information and data, including credit card information and other personally identifiable information, could cause interruptions in our operations and subject us to increased costs, litigation, inquiries and actions from governmental authorities, and financial or other liabilities. In addition, security breaches, incidents or the inability to protect information could lead to increased incidents of ticketing fraud and counterfeit tickets.
>
> . . . .
>
> We also face risks associated with security breaches and incidents affecting third parties with which we are affiliated or with which we otherwise conduct business. In particular, hardware, software or applications we develop or procure from third parties may contain, and have contained, defects in design or manufacture and/or may pose a security risk that could unexpectedly compromise information security, but none of which have been material to date.

---

[159] Live Nation, 2024 Annual Report (Form 10-K) at 17-18 (Feb. 22, 2024), https://investors.livenationentertainment.com/sec-filings/annual-reports/content/0001335258-24-000017/0001335258-24-000017.pdf.

401. Consumers, including the Ticketmaster Plaintiffs, relied upon or would be reasonable in relying upon Ticketmaster's express and implied commitments to protect the privacy of their Personal Information when they decided to utilize Ticketmaster's services.

402. Ticketmaster knew or should have known of the importance of oversight related to third-party providers. In 2018, Ticketmaster announced a data breach incident of a provider of AI-powered live chat widgets, which Ticketmaster was deploying on localized sites across the world.[160] This Data Breach was thus foreseeable because Ticketmaster dealt with a data breach involving a third-party provider in the past which did or reasonably should have put Ticketmaster on notice of its duty in reasonably selecting and overseeing third-party vendors it entrusted with customers' Personal Information.

IV. The Ticketmaster Defendants breached their duty to protect Personal Information and engaged in unfair trade practices.

403. Despite Ticketmaster's explicit assurances that it would employ reasonable measures to safeguard its customers' sensitive Personal Information, and only share that information with expressly authorized individuals, an

---

160 Catalin Cimpanu, *Ticketmaster Announces Data Breach Affecting 5% of All Users*, BleepingComputer (June 17, 2018), https://www.bleepingcomputer.com/news/security/ticketmaster-announces-data-breach-affecting-5-percent-of-all-users/.

"unauthorized" person or persons accessed Ticketmaster's network servers and reportedly stole the Personal Information they found.

404. Live Nation played a primary role investigating the Data Breach, disclosing in a Form 8-K filing to the U.S. Securities and Exchange Commission filed on May 31, 2024:

> On May 20, 2024, Live Nation Entertainment, Inc. (the "Company" or "we") identified unauthorized activity within a third-party cloud database environment containing Company data (primarily from its Ticketmaster L.L.C. subsidiary) and launched an investigation with industry-leading forensic investigators to understand what happened. On May 27, 2024, a criminal threat actor offered what it alleged to be Company user data for sale via the dark web. We are working to mitigate risk to our users and the Company, and have notified and are cooperating with law enforcement. As appropriate, we are also notifying regulatory authorities and users with respect to unauthorized access to personal information."[161]

405. Several months after the breach, on June 8, 2024, Ticketmaster disclosed the Data Breach to consumers in a notice, which the Ticketmaster Plaintiffs received.

406. In the Ticketmaster Notice, Ticketmaster represented the Data Breach occurred between April 2, 2024, and May 18, 2024, and that Ticketmaster had determined Personal Information was affected on May 23, 2024.

---

[161] Live Nation Entertainment, Inc., Current Report (Form 8-K) (May 20, 2024), https://www.sec.gov/Archives/edgar/data/1335258/000133525824000081/lyv-20240520.htm.

407. Ticketmaster also recommended that recipients, including the Ticketmaster Plaintiffs, "take steps to protect against identity theft and fraud," offered 1 year of free credit monitoring services, and made numerous additional recommendations to guard against identity fraud including:

> [W]e recommend you remain vigilant and take steps to protect against identity theft and fraud, including monitoring your accounts, account statements, and free credit reports for signs of suspicious activity. To further protect your identity and as a precaution, we are also offering you identity monitoring with TransUnion at no cost to you. Identity monitoring will look out for your personal data on the dark web and provide you with alerts for 1 year from the date of enrollment if your personally identifiable information is found online. . . .
>
> We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. . . .
>
> You should remain vigilant for incidents of fraud or identity theft by reviewing account statements and monitoring free credit reports. When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report. You should also call your local police department and file a report of identity theft. Finally, you should make sure to keep a copy of the police report in case you need to provide it to creditors or credit reporting agencies when accessing or disputing inaccurate information. . . .
>
> You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name

> without the use of a Personal Identification Number (PIN) that is issued to you when you initiate a freeze.[162]

408. However, Ticketmaster was vague as to the types of Personal Information compromised in the Data Breach and the number of affected consumers. The "Ticketmaster Data Security Incident" webpage describing the breach disclosed that it discovered "unauthorized activity on an isolated cloud database hosted by a third-party data services provider" and that the "database contained limited personal information of some customers who bought tickets to events in North America . . . . [which] may include email, phone number, encrypted credit card information as well as some other personal information provided to us."[163] Neither the Ticketmaster Notice nor Ticketmaster Data Security Incident webpage included any additional detail on the types of credit card information taken, nor did they include detail as to the number of total affected customers. And the Ticketmaster Notice was untimely, coming several months after the Breach itself.

---

[162] Ticketmaster Data Security Incident, https://help.ticketmaster.com/hc/en-us/articles/26110487861137-Ticketmaster-Data-Security-Incident (last visited Jan. 17, 2025).

[163] Ticketmaster, *Ticketmaster Data Security Incident*, https://help.ticketmaster.com/hc/en-us/articles/26110487861137-Ticketmaster-Data-Security-Incident (last visited Jan. 10, 2025).

409. At the time of the Data Breach, Ticketmaster failed to maintain reasonable data security measures and comply with FTC guidance, the PCI DSS, and other relevant industry standards summarized above. These data security failings included:

- Ticketmaster did not enforce MFA for its Snowflake accounts. Indeed, Ticketmaster chose to use Snowflake to store the Personal Information of millions of its customers despite knowing that Snowflake did not allow customers to enforce MFA.
- Ticketmaster did not rotate or disable the credentials of old Snowflake accounts.
- Ticketmaster did not implement network allow lists that restricted Snowflake account access to certain locations or trusted users.

410. Ticketmaster failed to take these actions despite its parent company, Live Nation, explicitly reporting that it faced data security risks just two months prior.

411. Ticketmaster further failed to properly investigate, retain, oversee and audit a competent cloud-based data storage provider, because Snowflake similarly had numerous data security failings, as described herein.

412. Ticketmaster's data security failings enabled the Data Breach. Without these basic protections, UNC5537 was able to exfiltrate the Personal Information of over 560 million Ticketmaster consumers with nothing more than stolen

Ticketmaster Snowflake credentials obtained through malware campaigns—and traffic the data to other cybercriminals.

413. Ticketmaster's failings were particularly egregious given the enormous amount of Personal Information it stored on Snowflake's servers. Tasked with handling the data of over 560 million consumers, Ticketmaster's failure to implement basic data security measures is all the more inexplicable and reckless.

414. Indeed, each of these basic protections could have prevented the Data Breach. For example:

- Had Ticketmaster implemented MFA, UNC5537 would not have been able to access Ticketmaster's data with just stolen credentials. MFA would have required an additional layer of authentication (i.e., a code sent via text message or email) that UNC5537 would not have had access to.

- Ticketmaster could have also prevented the Data Breach by maintaining a policy of rotating or disabling credentials that were either old or compromised in other data breaches. As the Mandiant Report found that a "majority of the credentials used by UNC5537" were available from historic malware campaigns dating back to 2020, a policy that disabled previously-compromised credentials could have prevented the Data Breach.[164]

- Ticketmaster could have also prevented the Data Breach by maintaining stricter network allow lists that restricted access to customer Personal Information to certain locations or trusted user accounts that were not previously compromised.

164 The Mandiant Report, *supra* n. 24.

415. In addition, Ticketmaster shirked the FTC Response Guidance by failing to give affected consumers sufficient information regarding the scale of the attack and the types of information taken in the Ticketmaster Notice.[165]

416. Ticketmaster, through these basic data security failings, breached its express representations in its Privacy Policy and Commitments. These representations included, but are not limited to, statements that Ticketmaster had implemented "security measures in place to protect [consumers'] information," would "ensure [consumers'] data was protected to the highest standard," and would "take all necessary security measures to protect personal information that's shared and stored with us."

417. In the alternative, Ticketmaster breached implied commitments to protect consumer Personal Information made to consumers, including the Ticketmaster Plaintiffs, by virtue of mandating that consumers provide their sensitive Personal Information as a condition of purchase.

418. Ticketmaster's basic data security failings also breached its duty of care to protect the Personal Information of consumers, which include the Ticketmaster Plaintiffs.

V. Personal Information stolen about Ticketmaster Plaintiffs and Class Members.

165 FTC Response Guidance, *supra* n. 56.

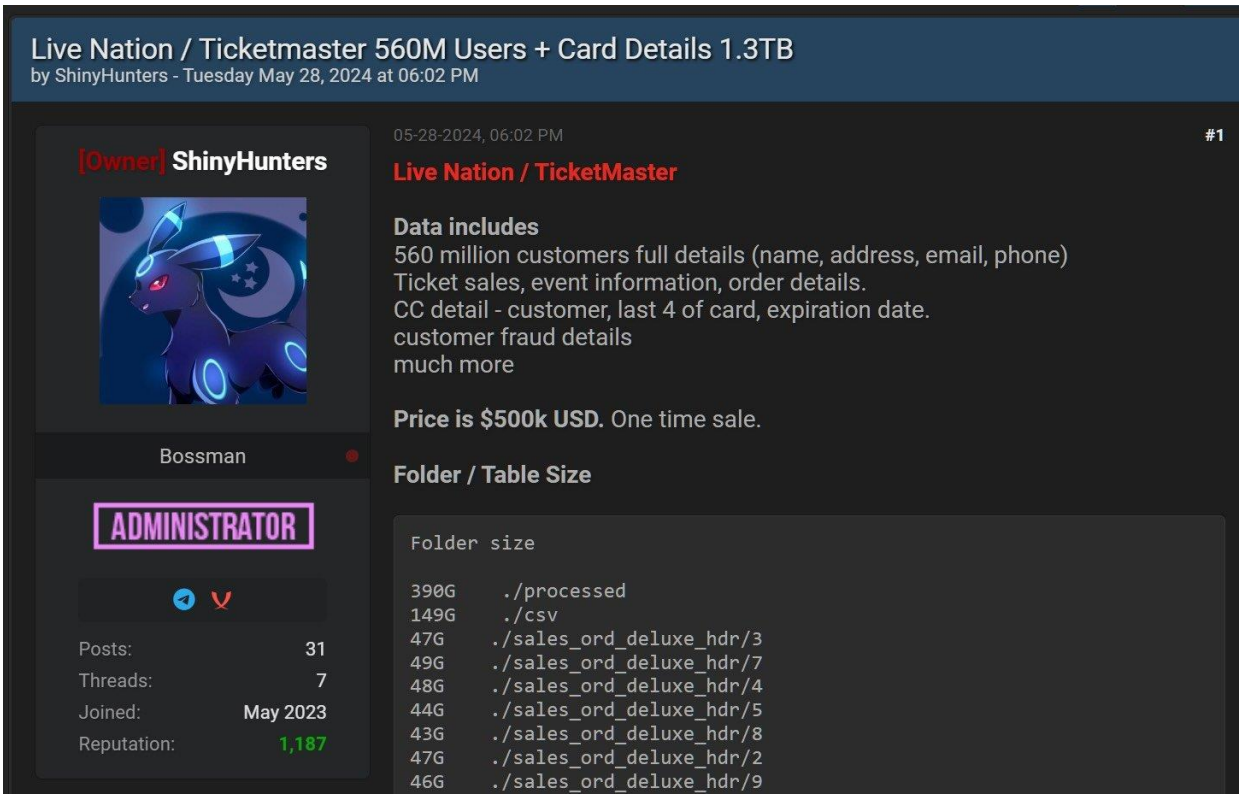
419. At a minimum, the stolen Personal Information about Ticketmaster customers included the identifiers disclosed in the Ticketmaster Notice, which informed customers that the information exposed in the Data Breach "may include email, phone number, encrypted credit card information as well as some other personal information provided to us."[166]

420. The stolen Personal Information also included names, addresses, emails, and phone numbers of Ticketmaster customers, as well as information regarding tickets they purchased through Ticketmaster, order confirmation details, and credit card information such as the last four digits of their payment cards and expiration dates. On May 28, 2024, around the time of the Data Breach, this very information was advertised for sale on a dark web forum post by a cybercriminal group by the name of "ShinyHunters" that claimed the information was stolen in the Snowflake Data Breach. A screenshot of this post is provided below.[167]

---

166 Ticketmaster, *Ticketmaster Data Security Incident*, https://help.ticketmaster.com/hc/en-us/articles/26110487861137-Ticketmaster-Data-Security-Incident (last visited Jan. 10, 2025)

167 Lawrence Abrams, *Ticketmaster confirms massive breach after stolen data for sale online*, Bleeping Computer (May 31, 2024), https://www.bleepingcomputer.com/news/security/ticketmaster-confirms-massive-breach-after-stolen-data-for-sale-online/.



421. While Ticketmaster represented in its Notice that the stolen credit card information was "encrypted," developments following the Data Breach call the veracity of Ticketmaster's statements into question.

422. For example, in December 2024, Visa issued over a hundred Compromised Account Management System ("CAMS") alerts to several credit unions. The CAMS alerts linked to a Ticketmaster press release and indicated that the breach compromised unique payment card numbers, along with data related to the payment card issuer and the cardholder account. In all, the CAMS alerts identified over a thousand payment cards compromised by the Data Breach. These CAMS alerts, together with Plaintiffs' allegations of attempted fraud and payment

card misuse, demonstrate that Ticketmaster's representations concerning the Data Breach may very well be confusing, incorrect, or blatantly misleading.[168]

423. In addition, the Data Breach compromised information relating to tickets purchased through Ticketmaster, which can also be used to perpetrate identity fraud. For example, as a threat, the cybercriminals leaked data for upcoming popular concerts and events that allowed fraudsters to effectively steal the ticket from a paying customer.[169]

VI. Ticketmaster Plaintiffs and Class Members suffered injuries as a result of the Data Breach.

424. As described herein, the Personal Information exposed in the Data Breach caused injury to the Ticketmaster Plaintiffs and Class Members.

425. First, the Data Breach subjected the Ticketmaster Plaintiffs and Class Members to a substantial risk of identity theft, which is demonstrated by facts including, but not limited to, incidences of fraud and attempted fraud suffered by

---

[168] To the extent that Plaintiffs discover that Ticketmaster's representations were inaccurate through discovery, they will respectfully seek leave to amend their complaint.

[169] Lawrence Abrams, *Hackers leak 39,000 print-at-home Ticketmaster tickets for 154 events*, Bleeping Computer (July 8, 2024), https://www.bleepingcomputer.com/news/security/hackers-leak-39-000-print-at-home-ticketmaster-tickets-for-154-events/; Jonathan Limehouse, *Scammers are accessing Ticketmaster users' email accounts, stealing tickets, company says*, USA Today (Oct. 1, 2024), https://www.usatoday.com/story/entertainment/music/2024/10/01/ticketmaster-scammers-disappearing-tickets/75470713007/.

the Plaintiffs, the posting of Ticketmaster Plaintiffs' and Class Members' Personal Information on the dark web, the inadequate vagueness of Ticketmaster's Notice as to Personal Information taken when compared against the specificity of Personal Information advertised for sale on the dark web, the sensitivity of Personal Information related to payment card data, CAMS alerts received by credit unions, and Ticketmaster's own Notice that expressly instructed affected customers to "take steps to protect against identity theft" and recommended that customers register for identity theft monitoring services. As a result of this substantial risk, Ticketmaster Plaintiffs and Class Members reasonably suffered injury in the form of lost time and resources mitigating against the risk of identity theft and emotional distress arising from the risk of identity theft.

426. Second, Ticketmaster made specific data security promises to Ticketmaster Plaintiffs and Class Members. Especially considering the high cost of tickets, a portion of the ticket price that Plaintiffs and Class Members paid to Ticketmaster would cover cybersecurity and protection of Personal Information. By exposing Personal Information to unauthorized third parties, Ticketmaster Plaintiffs and Class Members did not receive the benefit of their bargain. Additionally, Ticketmaster Plaintiffs and Class Members are entitled to damages for Ticketmaster's violation of contractual promises to them.

427. Third, Personal Information has inherent value, and the exposure of that information makes consumers susceptible to fraud and scams for years into the future. Not only should consumers be compensated for the value of their Personal Information, but they should also be provided with monitoring services to ensure that their data is not misused in the future.

VII. Class action allegations as to the Ticketmaster Defendants.

428. The Ticketmaster Plaintiffs brings this action on their own behalf, and on behalf the following Ticketmaster Class and Subclasses (the "Ticketmaster Classes").

- **Nationwide Ticketmaster Class.** All individuals residing in the United States who Ticketmaster and/or Live Nation identified as being among those individuals whose Personal Information was compromised in the Data Breach (the "Ticketmaster Class").
- **State-Specific Subclasses.** As described in this Section below, all individuals residing in a specific state who Ticketmaster and/or Live Nation identified as being among those individuals whose Personal Information was compromised in the Data Breach ("Ticketmaster Subclass").

429. Excluded from the Ticketmaster Classes are the Ticketmaster Defendants' officers and directors, any entity in which the Ticketmaster Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of the Ticketmaster Defendants. Excluded also from the Ticketmaster Classes are members of the judiciary to whom this case is assigned, their families and members of their staff.

430. The Ticketmaster Plaintiffs reserve the right to amend or modify the definition of the Ticketmaster Classes or create additional subclasses as this case progresses.

431. **Numerosity.** The members of the Ticketmaster Classes are so numerous that joinder of all of them is impracticable. Public reporting presently indicates that over 560 million Ticketmaster customers were affected by the Data Breach.

432. **Commonality.** There are questions of fact and law common to the Ticketmaster Classes, which predominate over individualized questions. These common questions of law and fact include, but are not limited to:

- Whether the Ticketmaster Defendants had a duty to protect the Personal Information of Ticketmaster Plaintiffs and Class Members.
- Whether the Ticketmaster Defendants breached express or implied commitments to protect the Personal Information of Ticketmaster Plaintiffs and Class Members.
- Whether the Ticketmaster Defendants knew or should have known that their data security practices were deficient.
- Whether the Ticketmaster Defendants' data security systems were consistent with industry standards prior to the Data Breach.
- Whether the Ticketmaster Defendants adequately disclosed details regarding the Data Breach to affected consumers.
- Whether the Ticketmaster Defendants unlawfully utilized, retained, misplaced, or exposed Plaintiffs' and the Class Members' Personal Information.

- Whether Ticketmaster Plaintiffs and Class Members are entitled to actual damages, punitive damages, treble damages, statutory damages, general damages, nominal damages, and/or injunctive relief.

433. **Typicality.** The Ticketmaster Plaintiffs' claims are typical of those of other Class Members because the Ticketmaster Plaintiffs' Personal Information, like that of every other Class Member, was compromised in the Data Breach

434. **Adequacy of Representation.** The Ticketmaster Plaintiffs will fairly and adequately represent and protect the interest of the Ticketmaster Class Members. Plaintiffs' Counsel are competent and experienced in litigating class actions.

435. **Predominance.** The Ticketmaster Defendants have engaged in a common course of conduct toward the Ticketmaster Plaintiffs and Class Members, in that all the data of Plaintiff and Class Members were stored on the same Snowflake Data Cloud network and unlawfully accessed in the same manner. The common issues arising from the Ticketmaster Defendants' conduct affecting Class Members listed above predominate over any individualized issues. Adjudication of these common issues in a single action will advance judicial economy.

436. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of the claims of the Ticketmaster Class. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Ticketmaster Class

Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Ticketmaster Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for the Ticketmaster Defendants. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Ticketmaster Class Member.

437. **Injunctive Relief.** The Ticketmaster Defendants have acted on grounds that apply generally to the Ticketmaster Class as a whole such that class certification, injunctive relief, and declaratory relief are appropriate on a class-wide basis.

438. **Issue Certification.** Likewise, particular issues are appropriate for certification because such claims present common issues whose resolution would advance the disposition of this matter. Such issues include, but are not limited to:

- Whether the Ticketmaster Defendants owed a legal duty to the Ticketmaster Plaintiffs and Class Members to protect their Personal Information.
- Whether the Ticketmaster Defendants' data security measures were inadequate in light of applicable regulations and industry standards.
- Whether the Ticketmaster Defendants' data security measures were negligent.

- Whether the Ticketmaster Defendants breached express or implied representations to the Ticketmaster Plaintiffs and Class Members regarding the protection of their Personal Information.

439. **Identification of Class Members Using Objective Criteria.** Finally, all members of the proposed Ticketmaster Classes are readily identifiable using objective criteria. The Ticketmaster Defendants have access to the names and contact information of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by the Ticketmaster Defendants.

VIII. Causes of action as to the Ticketmaster Defendants.

FIRST CLAIM FOR RELIEF
Negligence
On behalf of the Ticketmaster Plaintiffs and the Ticketmaster Class

440. The Ticketmaster Plaintiffs repeat and re-allege the allegations contained in Paragraphs 1 through 150, as well as Part One and Part Three, as set forth fully herein.

441. The Ticketmaster Defendants owed a duty under common law to the Ticketmaster Plaintiffs and Ticketmaster Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, and deleting their Personal Information in its possession from being compromised, stolen, or misused by unauthorized persons.

442. Specifically, this duty included, among other things: (a) implementing industry standard data security safeguards to protect the Personal Information of Ticketmaster Plaintiffs and Ticketmaster Class Members such as MFA, rotating credentials, and restricting access privileges; (b) maintaining, testing, and monitoring Ticketmaster's security systems to ensure that Personal Information was adequately secured and protected; (c) timely acting upon warnings and alerts to respond to intrusions; and (d) adequately notifying the Ticketmaster Plaintiffs and Ticketmaster Class Members about the types of data that were compromised in the Data Breach.

443. The Ticketmaster Defendants' duty to use reasonable care arose from several sources, including those set out below.

444. The Ticketmaster Defendants had a common law duty to prevent foreseeable harm to others. This duty existed because the Ticketmaster Defendants collected and stored valuable Personal Information that is routinely targeted by cyber criminals, and Ticketmaster had already experienced a data breach before. The Ticketmaster Plaintiffs and Ticketmaster Class Members were the foreseeable and probable victims of any compromise to inadequate data security practices maintained by Ticketmaster.

445. The Ticketmaster Defendants further assumed a duty of reasonable care in promulgating their Privacy Policy and Privacy Commitments which assured

the Ticketmaster Plaintiffs and Ticketmaster Class Members that their Personal Information would be adequately secured.

446. The Ticketmaster Defendants breached their duties owed to the Ticketmaster Plaintiffs and Ticketmaster Class Members by failing to maintain adequate data security practices that conformed with industry standards, and were therefore negligent.

447. The Ticketmaster Defendants breached their duties owed to Ticketmaster Plaintiffs and Ticketmaster Class Members by failing to exercise reasonable oversight in the selection of Snowflake to store Personal Information. Such reasonable oversight would have revealed that Snowflake's cloud services lacked industry standard data security safeguards necessary to adequately protect Personal Information.

448. The Data Breach was entirely foreseeable. Not only did industry experience show that a failure to adopt the security standards as described herein would result in data breaches, but the Ticketmaster Defendants, themselves, previously experienced a prior breach of a third-party provider by not exercising sufficient oversight over that entity

449. But for Ticketmaster's negligence, the Personal Information of the Ticketmaster Plaintiffs and Ticketmaster Class Members would not have been stolen by cybercriminals in the Data Breach.

450. As a direct and proximate result of the Ticketmaster Defendants' breach of duties, the Ticketmaster Plaintiffs and Ticketmaster Class Members have suffered injuries detailed above.

451. Plaintiffs and Ticketmaster Class Members are entitled to damages, including compensatory, general, nominal, and/or punitive damages, in an amount to be proven at trial.

SECOND CLAIM FOR RELIEF
Breach of Express Contract
On behalf of the Ticketmaster Plaintiffs and the Ticketmaster Class

452. The Ticketmaster Plaintiffs repeat and re-allege the allegations contained in Paragraphs 1 through 150, as well as Part One and Part Three, as set forth fully herein.

453. The Ticketmaster Defendants entered into a valid and enforceable contract with the Ticketmaster Plaintiffs and Ticketmaster Class Members.

454. That contract required the Ticketmaster Plaintiffs and Ticketmaster Class Members to provide their Personal Information in exchange for ticketing services.

455. While the contract was solely obtained because of the Ticketmaster Defendants' monopoly, promises that the Ticketmaster Defendants made to consumers are enforceable, even if unconscionable provisions are not. That contract

included by promises by the Ticketmaster Defendants to secure and safeguard the Ticketmaster Plaintiffs' and Ticketmaster Class Members' Personal Information.

456. The Ticketmaster Defendants' Privacy Policy and Privacy Commitments memorialized the obligations that the Ticketmaster Defendants had to protect the Ticketmaster Plaintiffs' and Ticketmaster Class Members' Personal Information.

457. The Ticketmaster Plaintiffs and Ticketmaster Class Members fully performed their obligations under their contracts with the Ticketmaster Defendants. However, the Ticketmaster Defendants failed to secure and safeguard their Personal Information, thus breaching contractual obligations.

458. The Ticketmaster Defendants' failure to secure and safeguard the Ticketmaster Plaintiffs' and Ticketmaster Class Members' Personal Information resulted in services that were of a diminished value and in breach of contractual obligations to the Ticketmaster Plaintiffs and Ticketmaster Class Members.

459. As a direct and proximate result of the Ticketmaster Defendants' breach of express contract, the Ticketmaster Plaintiffs and Ticketmaster Class Members have suffered injuries detailed above.

460. As a direct and proximate result of the Ticketmaster Defendants' breach of express contract, the Ticketmaster Plaintiffs and Ticketmaster Class Members are entitled to damages, including compensatory damages, general

damages, nominal damages, and/or punitive damages, in an amount to be proven at trial.

THIRD CLAIM FOR RELIEF
Breach of Implied Contract
On behalf of the Ticketmaster Plaintiffs and the Ticketmaster Class

461. The Ticketmaster Plaintiffs repeat and re-allege the allegations contained in Paragraphs 1 through 150, as well as Part One and Part Two, as set forth fully herein, in the alternative to the Ticketmaster Plaintiffs' breach of express contract claim, in the event a written agreement is unenforceable or deemed to not exist.

462. As a condition of using Ticketmaster's platform, the Ticketmaster Defendants required the Ticketmaster Plaintiffs and Ticketmaster Class Members to provide their Personal Information as a condition of use.

463. By mandating that Ticketmaster Plaintiffs and Ticketmaster Class Members provide their Personal Information as a condition of use, the Ticketmaster Defendants implied an assent to safeguard and protect their Personal Information.

464. The Ticketmaster Plaintiffs and Ticketmaster Class Members would not have provided their Personal Information to the Ticketmaster Defendants had they known that they would not safeguard their Personal Information as promised.

465. The Ticketmaster Plaintiffs and Ticketmaster Class Members fully performed their obligations under their implied contracts with the Ticketmaster Defendants.

466. The Ticketmaster Defendants breached their implied contracts with the Ticketmaster Plaintiffs and Ticketmaster Class Members by failing to safeguard their Personal Information.

467. As a direct and proximate result of the Ticketmaster Defendants' breach of implied contract, the Ticketmaster Plaintiffs and Ticketmaster Class Members have suffered injuries detailed above.

468. As a direct and proximate result of the Ticketmaster Defendants' breach of implied contract, the Ticketmaster Plaintiffs and Ticketmaster Class Members are entitled to damages, including compensatory damages, punitive damages, and/or nominal damages, in an amount to be proven at trial.

FOURTH CLAIM FOR RELIEF
Violation of the Montana Unfair Trade Practices & Consumer Protection Act (Mont. Code Ann. § 30-14-101, *et seq.*) ("MUTPCPA")
On behalf of Plaintiffs Madden and Murphy and the Montana Ticketmaster Subclass

469. Plaintiffs Madden and Murphy repeat and re-allege the allegations contained in Paragraphs 1 through 150, as well as Part One and Part Three, as set forth fully herein.

470. Plaintiffs Madden, Murphy, and Montana Ticketmaster Subclass Members are "consumers" under the MUTPCPA because they purchased ticketing services for personal, family, or household purposes. Mont. Code Ann. § 30-14-102(1).

471. The Ticketmaster Defendants are "persons" under the MUTPCPA, which are defined to mean "natural persons, corporations, trusts, partnerships, incorporated or unincorporated associations, and any other legal entity." Mont. Code Ann. § 30-14-102(6).

472. The Ticketmaster Defendants engaged in "trade" and "commerce" as defined by the MUTPCPA because their ticketing services were advertised and sold to Montana residents, including Plaintiff Maddens, Murphy, and Montana Ticketmaster Subclass Members. Mont. Code Ann. § 30-14-102(8)(a).

473. The Ticketmaster Defendants engaged in unfair and deceptive practices prohibited by the MUTPCPA. Mont. Code Ann. § 30-14-103.

474. The Ticketmaster Defendants engaged in unfair trade practices when it failed to maintain reasonable data security practices to safeguard the Personal Information of Plaintiff Madden and the Montana Ticketmaster Subclass, including: (a) failing to implement industry standard data security safeguards to protect consumer Personal Information such as MFA, rotating credentials, and restricting access privileges; (b) failing to maintain, test, and monitor the Ticketmaster

Defendants security systems to ensure that Personal Information was adequately secured and protected; (c) failing to timely act upon warnings and alerts to respond to intrusions; and (d) failing to adequately notify consumers about the types of data that were compromised in the Data Breach.

475. The Ticketmaster Defendants' conduct offends established public policy and is immoral, unethical, oppressive, unscrupulous and substantially injurious to consumers.

476. The Ticketmaster Defendants' conduct was also an unlawful deceptive trade practice because they represented to Plaintiffs Madden, Murphy, and the Montana Ticketmaster Subclass in their Privacy Policy and Privacy Commitments that consumer Personal Information mandated as a condition of purchase would be safeguarded and secured.

477. These representations were deceptive because, in fact, the Ticketmaster Defendants failed to maintain reasonable data security practices, which is demonstrated by failures including, but not limited to: (a) failing to implement industry standard data security safeguards to protect consumer Personal Information such as MFA, rotating credentials, and restricting access privileges; (b) failing to maintain, test, and monitor the Ticketmaster Defendants security systems to ensure that Personal Information was adequately secured and protected; (c) failing to timely act upon warnings and alerts to respond to intrusions; and (d)

failing to adequately notifying consumers about the types of data that were compromised in the Data Breach.

478. Plaintiffs Madden, Murphy, and Montana Ticketmaster Subclass Members members have suffered injury as a result of the Ticketmaster Defendants' unfair and deceptive trade practices, as described herein.

479. As a direct and proximate result of the Ticketmaster Defendants' deceptive acts, Plaintiffs Madden, Murphy, and the Montana Ticketmaster Subclass Members are entitled to injunctive relief, damages, including actual damages in an amount to be proven at trial or statutory damages of $500, whichever is greater, treble damages of actual damages, and reasonable attorneys' fees. Mont. Code Ann. § 30-14-133.

FIFTH CLAIM FOR RELIEF
Violation of New York General Business Law § 349 ("NYGBL § 349")
On behalf of Plaintiffs Anderson and Fitzgerald
and the New York Ticketmaster Subclass

480. Plaintiffs Anderson and Fitzgerald repeat and re-allege the allegations contained in Paragraphs 1 through 150, as well as Part One and Part Three, as set forth fully herein.

481. The Ticketmaster Defendants engaged in deceptive practices by representing to Plaintiffs Anderson, Fitzgerald, and the New York Ticketmaster Subclass in its Privacy Policy and Privacy Commitments that consumer Personal Information mandated as a condition of use would be safeguarded and secured.

482. These representations were deceptive because, in fact, the Ticketmaster Defendants failed to maintain reasonable data security practices, which is demonstrated by failures including, but not limited to: (a) failing to implement industry standard data security safeguards to protect consumer Personal Information such as MFA, rotating credentials, and restricting access privileges; (b) failing to maintain, test, and monitor the Ticketmaster Defendants' security systems to ensure that Personal Information was adequately secured and protected; (c) failing to timely act upon warnings and alerts to respond to intrusions; and (d) failing to adequately notifying consumers about the types of data that were compromised in the Data Breach.

483. Ticketmaster has suffered at least one other large Data Breach and failed to exercise sufficient oversight over a third-party data provider. Based upon the prior breach, another potential data breach was foreseeable or Ticketmaster was reckless in not foreseeing another potential data breach.

484. The Ticketmaster Defendants engaged in these deceptive acts in the conduct of business, trade, or commerce, and the furnishing of ticketing service in New York to New York consumers, which include Plaintiffs Anderson, Fitzgerald, and the New York Ticketmaster Subclass.

485. Plaintiffs Anderson, Fitzgerald, and the New York Ticketmaster Subclass have suffered injury as a result of the Ticketmaster Defendants' deceptive acts in the manners described above.

486. As a direct and proximate result of the Ticketmaster Defendants' deceptive acts, Plaintiffs Anderson, Fitzgerald, and the New York Ticketmaster Subclass are entitled to injunctive relief, damages, including actual damages in an amount to be proven at trial or statutory damages of $50, whichever is greater, treble damages of actual damages, and reasonable attorneys' fees.

SIXTH CLAIM FOR RELIEF
Violation of District of Columbia Consumer Protection Procedures Act, D.C. Code § 28-3901, *et* seq. ("D.C. CPPA")
On behalf of Plaintiff D. Thomas and the District of Columbia Ticketmaster Subclass

487. Plaintiff D. Thomas repeats and re-alleges the allegations contained in Paragraphs 1 through 150, as well as Part One and Part Three, as set forth fully herein.

488. A violation of the Washington D.C. Security Breach Protection Amendment Act of 2020 ("D.C. SBPAA"), including D.C. Code § 28-3852, constitutes a per se unfair or deceptive trade practice under the D.C. CPPA. *See* D.C. Code § 28-3853.

489. D.C. Code § 28-3852.01 of the D.C. SBPAA provides: "To protect personal information from unauthorized access, use, modification, disclosure, or a reasonably anticipated hazard or threat, a person or entity that owns, licenses, maintains, handles, or otherwise possesses personal information of an individual residing in the District shall implement and maintain reasonable security safeguards, including procedures and practices that are appropriate to the nature of the personal information and the nature and size of the entity or operation."

490. The Ticketmaster Defendants violated the D.C. SBPAA, and therefore the D.C. CPPA, by (a) failing to implement industry standard data security safeguards to protect consumer Personal Information such as MFA, rotating

credentials, and restricting access privileges; (b) failing to maintain, test, and monitor the Ticketmaster Defendants security systems to ensure that Personal Information was adequately secured and protected; (c) failing to timely act upon warnings and alerts to respond to intrusions; and (d) failing to adequately notify consumers about the types of data that were compromised in the Data Breach.

491. The Ticketmaster Defendants' actions were reckless. As a direct and proximate result of its security failures, Plaintiff D. Thomas and the Subclass Members' Personal Information was subject to unauthorized access and exfiltration, theft, and/or disclosure.

492. In addition to its per se violation of the D.C. CPPA, Ticketmaster engaged in unfair trade practices prohibited by the D.C. CPPA. D.C. Code § 28-3904.

493. Plaintiff D. Thomas and D.C. Ticketmaster Subclass Members are "consumers" under the D.C. CPPA because they "receive[d] consumer services" or "otherwise provide[d] the economic demand for a trade practice." D.C. Code § 28-3901(a)(2).

494. The Ticketmaster Defendants are "merchants" under the D.C. CPPA because they "supply the goods or services which are . . . the subject of a trade practice." D.C. Code § 28-3901(a)(3).

495. The Ticketmaster Defendants' services are "trade practices" because they are acts that "directly or indirectly . . . effectuate, a sale, lease or transfer, of consumer goods or services." D.C. Code § 28-3901(a)(6).

496. The Ticketmaster Defendants' conduct offends established public policy and is immoral, unethical, oppressive, unscrupulous and substantially injurious to consumers. The harm done sufficiently outweighs any justifications or motives for Ticketmaster's practice of collecting and storing Personal Information without appropriate and reasonable safeguards to protect such information in place. Consumers could not have reasonably avoided the harm inflicted by Ticketmaster.

497. As a result of Ticketmaster's violations of the D.C. CPPA, Plaintiff D. Thomas and D.C. Ticketmaster Subclass Members have suffered and will suffer injury, as described above.

498. As a direct and proximate result of the Ticketmaster Defendants' unlawful and unfair trade practices, Plaintiff Thomas and D.C. Ticketmaster Subclass Members are entitled to injunctive relief, damages, including actual damages in an amount to be proven at trial or statutory damages of $1,500, whichever is greater, treble damages of actual damages, and reasonable attorneys' fees. D.C. Code § 28-3905(k)(1)(A), (k)(2).

PART FOUR: ADVANCE AUTO PARTS AND ADVANCE STORES COMPANY

499. Plaintiffs Emmanuel Chaidez, Stefondra Monroe, Raymond Moule, Raven Richardson, Don Smith, and Raymond Swain (collectively, the "Advance Auto Plaintiffs") are named in this Representative Complaint to pursue claims against Advance Auto.[170]

I. The Advance Auto Defendants collect and store Personal Information of job applicants.

500. Advance Auto Parts, Inc. is a provider of automotive aftermarket parts. Advance Stores Company is a wholly owned subsidiary of Advance Auto.[171]

501. As of October 5, 2024, Advance Auto operated 4,781 stores primarily within the United States, with additional locations in Canada, Puerto Rico and the U.S. Virgin Islands.[172]

502. In the ordinary course of its business practices, Advance Auto collects, stores, and uses Plaintiffs' and Class Members' Personal Information.

---

[170] Advance Auto Parts, Inc. and Advance Stores Company, Inc. are collectively referred to herein, except as expressly delineated, as "Advance Auto" or the "Advance Auto Defendants."

[171] Advance Auto 2023 10-K, https://www.sec.gov/ix?doc=/Archives/edgar/data/1158449/000115844924000128/aap-20231230.htm.

[172] Advance Auto Parts, *The Advance Auto Parts Story*, https://corp.advanceautoparts.com/our-story/default.aspx (last visited Jan. 17, 2025).

503. Advance Auto collects Personal Information as part of its job application process, which include applicants' Social Security numbers, names, and dates of birth.[173]

504. Advance Auto maintains a privacy policy website, which states, "We need to collect Personal Information to provide the requested Services to you. If you do not provide the information requested, we may not be able to provide the Services."[174]

505. Advance Auto gains access to job applicant and employee Personal Information through various means, including its websites, its software applications, phone calls, and in-person business interactions at their stores.[175]

506. Advance Auto was a Snowflake customer. Snowflake was Advance Auto's cloud storage and data warehousing vendor.

507. Advance Auto stored consumer, applicant, and employee Personal Information on the Data Cloud.

II. The Advance Auto Defendants owed a duty of care to Plaintiffs and Class Members.

---

173 Advance Auto Parts, *Privacy Policy (Updated)* (Dec. 31, 2023) ("Advance Auto, *Privacy Policy*"), https://shop.advanceautoparts.com/o/privacy-notice?msockid=38767612e55363b5170c62f2e4e6626f.

174 Advance Auto, *Privacy Policy*.

175 *Id.*

508. Advance Auto also had obligations created by industry standards, common law, statutory law, and its own assurances and representations to keep Personal Information of Plaintiffs and the Class confidential and to protect such Personal Information from unauthorized access.

509. Advance Auto, in collecting Personal Information from job applicants, including the Advance Auto Plaintiffs, owed a duty to exercise reasonable care in maintaining, protecting, and securing their Personal Information. This duty arose under both federal and state law, as discussed herein, but also based upon industry standards.

510. Advance Auto collected sensitive Personal Information from its employees and job applicants as a condition of their application for employment with the company, and it was reasonably foreseeable that a data breach would subject those individuals to significant harm, given the sensitivity of the information collected. Accordingly, Advance Auto owed a duty to employees and applicants to adopt reasonable cybersecurity measures to keep their information secure, design systems and cloud-based computing applications that would keep information secure, monitor for known cybersecurity risks and threats, implement safeguards to protect systems from cybersecurity threats, engage in appropriate data management and hygiene, and take all other measures to safeguard employee and applicant information.

511. Advance Auto owed a duty to Plaintiffs and the Class to disclose if its computer systems and data security practices were inadequate to safeguard individuals' Personal Information from theft because such an inadequacy would be a material fact in the decision to entrust Personal Information with Advance Auto. Further, Advance Auto owed a duty to Plaintiffs and the Class to disclose in a timely and accurate manner when data breaches occurred.

512. Advance Auto itself suffered a prior data breach of sensitive employee information in 2016 and was therefore well aware of the security risks that maintaining such information posed. It should have taken basic cybersecurity steps to protect such information. As a result of that prior data breach, Advance Auto entered into a class action settlement agreement, where it agreed to a battery of "data security practices" with no sunset provision. *See Whitehead v. Advance Stores Company Inc.*, No. 5:16-cv-250-RBD-PRL (M.D. Fla.) (Doc. No. 40-1) (granted final approval on May 24, 2017).

513. Advance Auto should certainly have been aware, and indeed was aware, that it was at risk for a data breach that could expose the Personal Information that it collected and maintained.

514. Advance Auto was on notice of the importance of data encryption of Personal Information. Advance Auto knew it kept Personal Information of

consumers, applicants, and employees in its systems, but did not encrypt these systems or the information contained within them.

515. Advance Auto affirmatively represented to consumers and job applicants, "We seek to use reasonable organizational, technical, and administrative measures to protect Personal Information within our organization."[176]

516. In its Annual Report dated March 12, 2024, Advance Auto recognized data privacy among the risks facing the company. It stated[177]:

> The nature of our business requires us to receive, retain and transmit certain personally identifiable information about our customers, suppliers and team members, some of which is entrusted to third-party service providers. … Additionally, since we do not control our third-party service providers and our ability to monitor their data security is limited, we cannot ensure the security measures they take will be sufficient to protect our data. A weakness or failure or a breach of a third-party provider's software or systems or controls could result in the compromise of the confidentiality, integrity or availability of our systems or the data housed in our third-party solutions.
>
> Despite our efforts, our security measures may be breached in the future due to a cyber attack, computer malware viruses, exploitation of hardware and software vulnerabilities, team member error, malfeasance, fraudulent inducement (including so-called "social engineering" attacks and "phishing" scams) or other acts. While we have experienced threats to our data and systems, including phishing attacks, to date we are not aware that we have experienced a material cyber-security incident.

---

176 Advance Auto Parts, *Privacy Policy*.

177 Advance Auto 2023 10-K, https://www.sec.gov/ix?doc=/Archives/edgar/data/1158449/000115844924000128/aap-20231230.htm.

517. Prospective employees, including the Advance Auto Plaintiffs, relied upon Advance Auto's express and implied commitments to protect the privacy of their Personal Information when they decided to use Advance Auto's goods and services.

518. It was reasonably foreseeable to Advance Auto that failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and the Class Members' Personal Information—by not designing, adopting, implementing, controlling, directing, overseeing, managing, monitoring, and auditing appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems—would result in the release, disclosure, and dissemination of Plaintiffs' and the Class Members' Personal Information to unauthorized individuals.

III. The Advance Auto Defendants breached their duty to protect Plaintiffs' and Class Members' Personal Information.

519. On May 23, 2024, Advance Auto detected suspicious activity on its computer network, indicating a data breach.

520. Based on a subsequent forensic investigation, Advance Auto determined that cybercriminals infiltrated its inadequately secured computer systems and thereby gained access to its data files.

521. In a July 10, 2024 breach notification letter, Advance Auto stated, "an unauthorized third party accessed or copied certain information maintained by Advance Auto Parts from April 14, 2024, to May 24, 2024."[178]

522. According to information Advance Auto provided to the Maine Office of the Attorney General, cybercriminals potentially accessed and acquired files containing the sensitive personal information of 2,316,591 individuals through this infiltration.[179]

523. The personal information accessed by cybercriminals involved a wide variety of Personal Information, including names, dates of birth, Social Security numbers, driver's license numbers, and government identification numbers.

524. Advance Auto failed to spend sufficient resources on preventing external access to this highly sensitive information, failed to develop systems to detect outside infiltration, and further inadequately trained its employees to identify malware threats and defend against them.

525. At the time of the Data Breach, Advance Auto failed to maintain reasonable data security measures and comply with FTC guidance and other

---

178 Advance Auto Notice, *supra* n. 77.

179 *Data Breach Notifications*, *Advance Stores Company, Inc.*, Me. Att'y Gen. Off., https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/9a6279ea-12a4-47c8-855e-9ce509f5a2b2.html (last visited Jan. 17, 2025).

relevant industry standards summarized above. These data security failings included:

- Advance Auto did not enforce MFA for its Snowflake accounts.
- Advance Auto did not rotate or disable the credentials of old Snowflake accounts.
- Advance Auto did not implement network allow lists that restricted Snowflake account access to certain locations or trusted users.

526. Advance Auto failed to take these measures despite being under constant and attempted attacks from threat actors.

527. Advance Auto further failed to properly investigate, retain, oversee and audit a competent cloud-based data storage provider, because Snowflake similarly had numerous data security failings, as described herein.

528. Advance Auto's data security failings enabled the Data Breach. Without these basic protections, the threat actor was able to exfiltrate the Personal Information of millions of applicants and employees with nothing more than stolen Advance Auto or Snowflake credentials.

529. Indeed, each of these basic protections could have prevented the Data Breach. For example:

- Had Advance Auto implemented MFA, the threat actor would not have been able to access Advance Auto data with compromised or outdated credentials.

- Advance Auto could have also prevented the Data Breach by maintaining a policy of rotating or disabling credentials that were either old or compromised in other data breaches. As the Mandiant Report found that a "majority of the credentials used by UNC5537" were available from historic malware campaigns dating back to 2020, a policy that disabled previously-compromised credentials could have prevented the Data Breach.[180]

- Advance Auto could have also prevented the Data Breach by maintaining stricter network allow lists that restricted access to customer Personal Information to certain locations or trusted user accounts that were not previously compromised.

IV. Personal Information stolen about Advance Auto Plaintiffs and Class Members.

530. On or around July 10, 2024, Advance Auto provided individuals affected by the Data Breach with a Notice (the "Advance Auto Notice") that was printed on Advance Auto Parts letterhead. The letter defined the corporate entities "Advance Stores Company" and "Advance Auto Parts" interchangeably as follows: "Advance Stores Company, Incorporated ("Advance Auto Parts") writes to inform you of an incident that involves your personal information."[181]

531. The Notice disclosed, "an unauthorized third party gained access to certain information maintained by Advance Auto Parts within Snowflake, our cloud storage and data warehousing vendor." The Notice informed the recipient: "The personal information about you involved in this incident may include your name

180 The Mandiant Report, *supra* n. 24.

181 Advance Auto Notice, *supra* n. 77.

and the following: Social Security number, driver's license or other government issued identification number, and date of birth. This information was collected as part of the Advance Auto Parts job application process."[182]

532. The Notice offered affected individuals 12 months of free credit monitoring and identity restoration services and instructed individuals to "remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors over the next twelve (12) to twenty-four (24) months."[183]

533. This information regarding Advance Auto job applicants was packaged for sale on the dark web, together with information related to Advance Auto consumers.[184] On June 5, 2024, a cybercriminal group by the name of "Sp1d3r" advertised for sale a package of Advance Auto data linked with the Snowflake Data Breach, which included the Personal Information of employees and consumers. A screenshot of this post is provided below.[185]

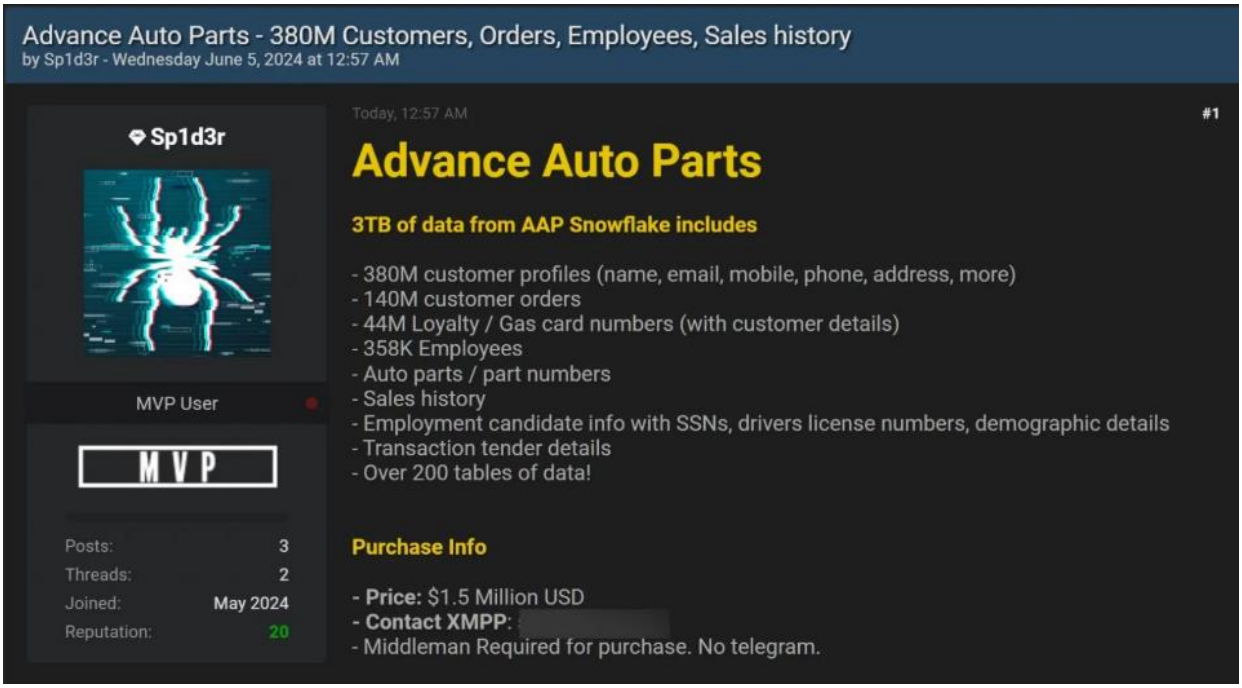
---

182 Advance Auto Notice, *supra* n. 77.

183 *Id.*

184 Lawrence Abrams, *Advance Auto Parts confirms data breach exposed employee information*, Bleeping Computer (June 19, 2024), https://www.bleepingcomputer.com/news/security/advance-auto-parts-confirms-data-breach-exposed-employee-information/.

185 *Id.*



534. Plaintiffs and Class Members have a privacy interest in the non-disclosure of their Social Security and driver's license numbers, as they are static identifiers that can be used to perpetrate identity fraud. This is especially the case where, as here, the Social Security and driver's license numbers are disclosed alongside other identifiers, including names, addresses, and contact information.

V. Plaintiffs and Class Members suffered injuries as a result of the Data Breach.

535. As described herein, the Personal Information exposed in the Data Breach caused injury to Advance Auto Plaintiffs and Class Members.

536. First, the Data Breach subjected Plaintiffs and Class Members to a substantial risk of identity theft, which is demonstrated by facts including, but not limited to, incidences of identity fraud suffered by the Advance Auto Plaintiffs, the

posting of Advance Auto Plaintiffs' and Class Members' Personal Information on the dark web, the inadequate vagueness of Advance Auto's Notice as to Personal Information taken when compared against the specificity of Personal Information advertised for sale on the dark web, the sensitivity of Personal Information related to Social Security numbers, driver's numbers, and other personal identifiers, and Advance Auto's own Notice that expressly instructed affected customers to "remain vigilant . . . by reviewing account statements and monitoring your free credit reports for suspicious activity" and recommending that customers register for credit monitoring services. As a result of this substantial risk, Advance Auto Plaintiffs and Class Members reasonably suffered injury in the form of lost time and resources mitigating against the risk of identity theft and emotional distress arising from the risk of identity theft.

537. Second, Advance Auto made specific express and implied data security representations to Advance Auto Plaintiffs and Class Members in the course of mandating receipt of applicants', employees', and consumers' Personal Information. By exposing Personal Information to unauthorized third parties in a manner inconsistent with these commitments and representations, Advance Auto Plaintiffs and Class Members did not receive the benefit of their bargain when they provided their Personal Information in exchange for employment or the purchase of goods.

538. Third, Personal Information has inherent value, and the exposure of that information makes employees and consumers susceptible to fraud and scams for years into the future. Not only should applicants, employees, and consumers be compensated for the value of their Personal Information, but they should also be provided with monitoring services to ensure that their data is not misused in the future.

539. Fourth, the disclosure of Advance Auto Plaintiffs' and Class Members' private and sensitive nature of the Personal Information to cybercriminals who in turn advertised and sold the Personal Information on the dark web, constitutes a privacy injury.

VI. Class action allegations as to the Advance Auto Defendants.

540. The Advance Auto Plaintiffs bring this action on their own behalf, and on behalf the following Advance Auto Class and Subclasses (the "Advance Auto Classes").

- **Nationwide Advance Auto Class.** All Advance Auto employees and employee applicants residing in the United States who Advance Auto identified as being among those individuals whose Personal Information was compromised in the Data Breach (the "Advance Auto Class").
- **State-Specific Subclasses.** As described in this Section below, all Advance Auto employees and employee applicants residing in a specific state who Advance Auto identified as being among those individuals whose Personal Information was compromised in the Data Breach ("Advance Auto Subclass").

- **California CCPA Subclass.** All individuals whose nonencrypted and nonredacted personal information, as defined in Cal. Civ. Code § 1798.150(a), was identified as compromised in the Data Breach by Advance Auto ("Advance Auto CCPA Subclass").

541. Excluded from the Advanced Auto Classes are Advance Auto's officers and directors, any entity in which Advance Auto has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Advance Auto. Excluded also from the Advance Auto are members of the judiciary to whom this case is assigned, their families and members of their staff.

542. The Advance Auto Plaintiffs reserve the right to amend or modify the definition of the Advance Auto Classes or create additional subclasses as this case progresses.

543. The proposed Classes meet the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

544. **Numerosity.** The members of the Advance Auto Classes are so numerous that joinder of all of them is impracticable. Public reporting presently indicates that over 560 million Advance Auto customers were affected by the Data Breach.

545. **Commonality.** There are questions of fact and law common to the Advance Auto Classes, which predominate over individualized questions. These common questions of law and fact include, but are not limited to:

- Whether Advance Auto had a duty to protect the Personal Information of Advance Auto Plaintiffs and Class Members.
- Whether Advance Auto breached express or implied commitments to protect the Personal Information of Advance Auto Plaintiffs and Class Members.
- Whether Advance Auto knew or should have known that their data security practices were deficient.
- Whether Advance Auto's data security systems were consistent with industry standards prior to the Data Breach.
- Whether Advance Auto adequately disclosed details regarding the Data Breach to affected consumers.
- Whether Advance Auto unlawfully utilized, retained, misplaced, or exposed Plaintiffs' and the Class Members' Personal Information.
- Whether Advance Auto Plaintiffs and Class Members are entitled to actual damages, punitive damages, treble damages, statutory damages, general damages, nominal damages, and/or injunctive relief.

546. **Typicality.** The Advance Auto Plaintiffs' claims are typical of those of other Class Members because the Advance Auto Plaintiffs' Personal Information, like that of every other Class Member, was compromised in the Data Breach

547. **Adequacy of Representation.** The Advance Auto Plaintiffs will fairly and adequately represent and protect the interest of the Advance Auto Class Members. Plaintiffs' Counsel are competent and experienced in litigating class actions.

548. **Predominance.** Advance Auto have engaged in a common course of conduct toward the Advance Auto Plaintiffs and Class Members, in that all the data of Plaintiff and Class Members were stored on the same Snowflake Data Cloud network and unlawfully accessed in the same manner. The common issues arising from Advance Auto's conduct affecting Class Members listed above predominate over any individualized issues. Adjudication of these common issues in a single action will advance judicial economy.

549. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of the claims of the Advance Auto Classes. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Advance Auto Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Advance Auto Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Advance Auto. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Advance Auto Class Member.

550. **Injunctive Relief.** Advance Auto has acted on grounds that apply generally to the Advance Auto Class as a whole such that class certification, injunctive relief, and declaratory relief are appropriate on a class-wide basis.

551. **Issue Certification.** Likewise, particular issues are appropriate for certification because such claims present common issues whose resolution would advance the disposition of this matter. Such particular issues include, but are not limited to:

- Whether Advance Auto owed a legal duty to the Advance Auto Plaintiffs and Class Members to protect their Personal Information.
- Whether Advance Auto's data security measures were inadequate in light of applicable regulations and industry standards.
- Whether Advance Auto's data security measures were negligent.
- Whether Advance Auto breached express or implied representations to the Advance Auto Plaintiffs and Class Members regarding the protection of their Personal Information.

552. **Identification of Class Members Using Objective Criteria.** Finally, all members of the proposed Advance Auto Classes are readily identifiable using objective criteria. Advance Auto have access to the names and contact information of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Advance Auto.

553. **Numerosity**: The proposed Class is believed to be so numerous that joinder of all members is impracticable. The proposed Subclass is also believed to be so numerous that joinder of all members would be impractical.

554. **Typicality**: Plaintiff's claims are typical of the claims of the Class. Plaintiffs and all members of the Class were injured through Defendants' uniform misconduct. The same event and conduct that gave rise to Plaintiff's claims are identical to those that give rise to the claims of every other Class member because Plaintiffs and each member of the Class had their sensitive Personal Information compromised in the same way by the same conduct of Defendants.

555. **Adequacy**: Plaintiffs are an adequate representative of the Class because their interests do not conflict with the interests of the Class and proposed Subclass that they seek to represent; Plaintiffs have retained counsel competent and highly experienced in data breach class action litigation; and Plaintiffs and Plaintiffs' counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and Plaintiffs' counsel.

556. **Superiority**: A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult, if not impossible, for members of the Class individually

to effectively redress Advance Auto's wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

557. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiffs and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

- Whether Advance Auto engaged in the wrongful conduct alleged herein;
- Whether Advance Auto failed to adequately safeguard Plaintiffs' and the Class's Personal Information;
- Whether Advance Auto's data security practices used to protect Plaintiffs' and Class Members' Personal Information violated the FTC Act, and/or state laws and/or Advance Auto's other duties discussed herein;
- Whether Advance Auto owed a duty to Plaintiffs and the Class to adequately protect their Personal Information, and whether it breached this duty;

- Whether Advance Auto knew or should have known that its computer and network security systems were vulnerable to a data breach;

- Whether Advance Auto breached contractual duties owed to Plaintiffs and the Class to use reasonable care in protecting their Personal Information;

- Whether Advance Auto failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiffs and the Class; and

- Whether Advance Auto continues to breach its duties to Plaintiffs and the Class.

VII. Causes of action as to the Advance Auto Defendants.

FIRST CLAIM FOR RELIEF
Negligence

On behalf of the Advance Auto Plaintiffs and the Advance Auto Class

558. The Advance Auto Plaintiffs repeat and re-allege the allegations contained in Paragraphs 1 through 150, as well as Part One and Part Four, as set forth fully herein.

559. The Advance Auto Defendants owed a duty under common law to the Advance Auto Plaintiffs and Advance Auto Class to exercise reasonable care in obtaining, retaining, securing, safeguarding, and deleting their Personal Information in its possession from being compromised, stolen, or misused by unauthorized persons.

560. The Advance Auto Defendants had a duty to implement industry standard data security safeguards to protect the Personal Information of Auto Plaintiffs and Advance Auto Class, such as MFA, rotating credentials, and restricting access privileges.

561. The Advance Auto Defendants had a duty to maintain, test, and monitor their security systems to ensure that Personal Information was adequately secured and protected.

562. The Advance Auto Defendants had a duty to timely act upon warnings and alerts to respond to intrusions.

563. The Advance Auto Defendants had a duty to adequately notify the Advance Auto Plaintiffs and Advance Auto Class about the types of data that were compromised in the Data Breach.

564. The Advance Auto Defendants had a common law duty to prevent foreseeable harm to others. This duty existed because the Advance Auto Defendants collected and stored valuable Personal Information that is routinely targeted by cybercriminals. The Advance Auto Plaintiffs and Advance Auto Class Members were the foreseeable and probable victims of any compromise to inadequate data security practices maintained by the Advance Auto Defendants.

565. Advance Auto Plaintiffs and Advance Auto Class Members were the foreseeable victims of any inadequate safety and security practices on the part of

the Advance Auto Defendants. Advance Auto Plaintiffs and Advance Auto Class Members had no ability to protect their Personal Information that was in Advance Auto Defendants' possession.

566. The Advance Auto Defendants further assumed a duty of reasonable care in promulgating their Privacy Policy which assured the Advance Auto Plaintiffs and Advance Auto Class Members that their Personal Information would be adequately secured.

567. The Advance Auto Defendants breached their duties owed to the Advance Auto Plaintiffs and Advance Auto Class Members by failing to maintain adequate data security practices that conformed with industry standards, and were therefore negligent.

568. The Advance Auto Defendants breached their duties owed to Advance Auto Plaintiffs and Class Members by failing to exercise reasonable oversight in the selection of Snowflake to store Personal Information. Such reasonable oversight would have revealed that Snowflake's cloud services lacked industry standard data security safeguards necessary to adequately protect Personal Information.

569. But for the Advance Auto Defendants' negligence, the Personal Information of the Advance Auto Plaintiffs and Advance Auto Class Members would not have been stolen by cybercriminals in the Data Breach.

570. As a direct and proximate result of the Advance Auto Defendants' negligence, the Advance Auto Plaintiffs and Advance Auto Class Members have suffered injuries detailed above.

571. As a direct and proximate result of the Advance Auto Defendants' negligence, the Advance Auto Plaintiffs and Advance Auto Class Members are entitled to damages, including compensatory, general, nominal, and/or punitive damages, in an amount to be proven at trial.

SECOND CLAIM FOR RELIEF
Breach of Implied Contract
On Behalf of the Advance Auto Plaintiffs and the Advance Auto Class

572. The Advance Auto Plaintiffs repeat and re-allege the allegations contained in Paragraphs 1 through 150, as well as Part One and Part Four, as set forth fully herein.

573. The Advance Auto Defendants required Advance Auto Plaintiffs and Advance Auto Class Members to provide their Personal Information as a condition of employment and/or applying for employment.

574. In mandating the Advance Auto Plaintiffs and Advance Auto Class Members to provide their Personal Information as a condition of employment and/or applying for employment, the Advance Auto Defendants implied an assent to safeguard and protect their Personal Information.

575. The Advance Auto Plaintiffs and Advance Auto Class would not have provided their Personal Information to Advance Auto if they had known that it would not safeguard their Personal Information.

576. The Advance Auto Plaintiffs and Advance Auto Class fully performed their obligations under the implied contracts with Advance Auto.

577. The Advance Auto Defendants breached their implied contracts with the Advance Auto Plaintiffs and Advance Auto Class by failing to safeguard their Personal Information.

578. The Advance Auto Defendants breached their implied contracts with the Advance Auto Plaintiffs and Advance Auto Class by failing to oversee its data storage vendor, Snowflake.

579. As a direct and proximate result of the Advance Auto Defendants' breach of implied contract, the Advance Auto Plaintiffs and Advance Auto Class Members suffered injuries detailed above.

580. As a direct and proximate result of the Advance Auto Defendants' breach of express contract, the Advance Auto Plaintiffs and Advance Auto Class are entitled to damages, including compensatory damages, general damages, nominal damages, and/or punitive damages, in an amount to proven at trial.

THIRD CLAIM FOR RELIEF
Violation of California Consumer Privacy Act
("CCPA") (Cal. Civ. Code § 1798.100)
On behalf of Plaintiff Swain and the Advance Auto CCPA Subclass

581. Plaintiff Swain repeats and re-alleges the allegations contained in Paragraphs 1 through 150, as well as Part One and Part Four, as set forth fully herein.

582. Cal. Civ. Code § 1798.150(a) of the CCPA provides that "[a]ny consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5 . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action" for statutory damages, actual damages, injunctive relief, declaratory relief and any other relief the court deems proper.

583. The Advance Auto Defendants solicited, gathered, and stored the Personal Information of Plaintiff Swain and the Advance Auto CCPA Subclass as part of the operation of its business.

584. The Advance Auto Defendants violated California Civil Code § 1798.150 of the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the Personal Information of California Plaintiffs and Advance Auto California Subclass Members. As a direct and proximate result of these security failures, Plaintiff Swain

and the Advance Auto CCPA Subclass Members' Personal Information was subject to unauthorized access and exfiltration, theft, or disclosure. This Personal Information included at least names, addresses, Social Security numbers, and driver's license numbers.

585. The Advance Auto Defendants are a "business" under the meaning of Cal. Civil Code § 1798.140 because they are a "corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners" that "collects consumers' personal information" and is active "in the State of California" and "had annual gross revenues in excess of twenty-five million dollars ($25,000,000) in the preceding calendar year." Cal. Civil Code § 1798.140(d).

586. Plaintiff Swain and Advance Auto CCPA Subclass Members are "consumers" as defined by Cal. Civ. Code § 1798.140(g) because they are natural persons who reside in California.

587. Plaintiff Swain and Advance Auto CCPA Subclass Members seek injunctive or other equitable relief to ensure Advance Auto hereinafter adequately safeguard their Personal Information by implementing reasonable security procedures and practices. Such relief is particularly important because the Advance Auto Defendants continue to hold Personal Information, including that of Plaintiff Swain and Advance Auto CCPA Subclass Members.

588. Plaintiff Swain and Advance Auto CCPA Subclass Members have an interest in ensuring that their Personal Information is reasonably protected, and Advance Auto has demonstrated a pattern of failing to adequately safeguard this information.

589. Notice related to Plaintiffs' intention to bring claims pursuant to the CCPA was sent to the Advance Auto Defendants on December 27, 2024. Despite receipt of the letter, the Advance Auto Defendants have refused to cure their violations as demanded by Plaintiffs.

590. The Advance Auto Defendants failed to take sufficient and reasonable measures to safeguard its data security systems and protect Plaintiff Swain and Advance Auto CCPA Subclass Members' Personal Information from unauthorized access. The Advance Auto Defendants' failure to maintain adequate data protections subjected Plaintiff Swain and Advance Auto CCPA Subclass Members' Personal Information to exfiltration and disclosure by malevolent actors.

591. The unauthorized access, exfiltration, theft, and disclosure of Plaintiff Swain and Advance Auto CCPA Subclass Members' Personal Information was a result of the Advance Auto Defendants' violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information.

592. The Advance Auto Defendants' unreasonable security practices include, but are not limited to: (a) failing to implement industry standard data security safeguards to protect the Personal Information of Advance Auto Plaintiffs and Class Members relating to MFA, rotating credentials, and restricting access privileges; (b) failing to maintain, test, and monitor Snowflake security systems to ensure that Personal Information was adequately secured and protected; (c) failing to implement intrusion detection systems and notifying customers of suspicious intrusions.

593. Plaintiff Swain and Advance Auto CCPA Subclass Members have suffered actual injury as detailed above, and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

594. The Advance Auto Defendants' violations of Cal. Civ. Code § 1798.150(a) are a direct and proximate cause of the Data Breach.

595. Plaintiff Swain and Advance Auto CCPA Subclass Members seek all monetary and non-monetary relief allowed by law, including actual, general, or nominal damages; declaratory and injunctive relief, including an injunction barring Advance Auto from disclosing their Personal Information without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper.

596. Plaintiff Swain and Advance Auto CCPA Subclass Members are further entitled to statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater. *See* Cal. Civ. Code § 1798.150(b).

597. As a result of the Advance Auto Defendants' failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiff Swain and Advance Auto CCPA Subclass Members seek actual damages, injunctive relief, including public injunctive relief, and declaratory relief, and any other relief as deemed appropriate by the Court.

PART FIVE: LENDINGTREE AND QUOTEWIZARD

598. Plaintiffs Aaron Macom, Antoun Nader, Linda Pierce, and Nathan Thomas (collectively, the "LendingTree Plaintiffs") are named in this Representative Complaint to pursue claims against LendingTree.[186]

I. The LendingTree Defendants' business and data security promises.

599. LendingTree is an online marketplace that aggregates terms for financial products, such as loans, credit cards, and insurance.

600. QuoteWizard is a wholly owned subsidiary of LendingTree, and is an online insurance marketplace that helps consumers compare quotes from agents and carriers for various insurance products. Consumers can use QuoteWizard to compare quotes for auto, home, renters, and health insurance. In providing such comparisons, QuoteWizard provides consumers with links to shop for insurance with various insurance companies.

601. In order to obtain an insurance comparison from QuoteWizard, consumers are required to provide QuoteWizard with highly sensitive personal information, including their full name, address, email address and phone number, date of birth, and motor vehicle information.

[186] LendingTree, LLC and Quotewizard.com, LLC are collectively referred to herein, except as expressly delineated, as "LendingTree" or the "LendingTree Defendants."

602. LendingTree describes itself as "the nation's leading online loan marketplace[.]"[187]

603. LendingTree acquired QuoteWizard in October 2018.[188]

604. QuoteWizard and LendingTree are highly integrated with respect to collecting customer Personal Information, sharing customer Personal Information and developing and implementing privacy policies. To provide several examples:

- When a consumer visits the QuoteWizard webpage, the prominently displayed QuoteWizard logo informs consumers that the company is called: "QuoteWizard by LendingTree."

- LendingTree and QuoteWizard maintain identical privacy policies that inform consumers that: "LendingTree, LLC, and its subsidiaries and affiliates (collectively, "LendingTree," "we," "our," or "us") are committed to maintaining your confidence and trust as it relates to the privacy and security of your personal information."[189]

- The privacy policies maintained by LendingTree and QuoteWizard list the identical LendingTree point of contact for consumers with privacy inquiries[190]:

---

187 *Our Brands*, LendingTree, https://press.lendingtree.com/about/our-brands (last visited Jan. 17, 2025).

188 Unaudited Pro Forma Condensed Combined Statement of Operations, https://www.sec.gov/Archives/edgar/data/1434621/000143462119000053/ex992.htm.

189 Privacy Policy, QuoteWizard by LendingTree, https://quotewizard.com/corp/privacy-policy (last updated Apr. 2, 2024) ("QuoteWizard, *Privacy Policy*").

190 *Id.*

- The identical privacy policies of both QuoteWizard and LendingTree explain: "We disclose your personal information to other entities within our family of brands to fulfill any purpose described in this Privacy Policy" and QuoteWizard is listed as part of that "family."[191]

605. In the ordinary course of its business, LendingTree collects, stores, and uses Plaintiffs' and Class Members' Personal Information.

606. LendingTree collects consumers' Personal Information as a condition of accessing its services.

607. LendingTree collects consumers' Personal Information, including names, addresses, telephone numbers, email addresses, account names, Social Security numbers, and dates of birth.[192]

608. LendingTree maintained a Privacy Policy which stated that it discloses consumers' personal information to "third parties that provide business, professional, or technical support services to us and/or administer activities on our behalf," but it did not identify these "Service Providers."[193]

---

191 *Id.*; Privacy Policy, LendingTree, https://www.lendingtree.com/legal/privacy-policy/ (last updated Apr. 2, 2024) ("Lending Tree, *Privacy Policy*"); *see also* Our Brands, LendingTree: Newsroom, https://press.lendingtree.com/about/our-brands (last accessed Dec. 20, 2024) (listing LendingTree and QuoteWizard).

192 Lending Tree, *Privacy Policy*.

193 *Id.*

609. LendingTree was a Snowflake customer. Snowflake was LendingTree's cloud storage and data warehousing vendor.

610. LendingTree stored consumers' Personal Information on the Data Cloud.

611. LendingTree represented in its Privacy Policy that it had several measures in place to safeguard consumers' Personal Information: "We maintain physical, electronic, and procedural measures designed to safeguard your personal information from unauthorized access and disclosure."[194]

612. LendingTree maintained a Security Policy on its website, in which it represented that it encrypted and protected consumers' information from third party interception[195]:

> **Security**
>
> While no data transmission over the Internet or information storage technology can be guaranteed to be 100% secure, LendingTree understands your concerns with the safety of your personal information.
>
> . . .
>
> **Secure Web Pages and Encryption**
>
> Transmissions between LendingTree, banks, lenders, loan brokers and real estate professionals (and affiliates) are encrypted using public key cryptography algorithms with a minimum key size of 128 bits.

---

194 *Id.*

195 Lending Tree, *Security Policy*, https://web.archive.org/web/20240405224851/https://www.lendingtree.com/legal/security/ (archived Apr. 5, 2024).

> SSL secures and prevents third parties from intercepting and reading your personal information; only we can decode the encryption. . . .
>
> Our website will log you out after a specified period of inactivity. This ensures your account security if you forget to logout from our website.

613. LendingTree further represented in its Security Policy that its firewalls protected consumer data from "external threats"[196]:

> **Firewall Protection**
>
> Firewalls are special purpose devices that protect and screen-out malicious attempts to access information and networks. LendingTree deploys Next Generation Firewalls to protect our resources and consumer data from internal and external threats.

II. The LendingTree Defendants owed a duty of care to Plaintiffs and Class Members.

614. LendingTree had obligations created by industry standards, common law, statutory law, and its own assurances and representations that it would keep Personal Information of Plaintiffs and the Class confidential and that it would protect such Personal Information from unauthorized access.

615. LendingTree, in collecting such sensitive Personal Information from consumers, owed a duty of care to consumers, including the LendingTree Plaintiffs, to exercise reasonable care in maintaining, protecting, and securing their Personal Information.

196 *Id.*

616. By mandating the receipt of sensitive Personal Information from consumers as a condition of providing insurance quote services, LendingTree implied its assent to consumers to protect their Personal Information. Consumers expected LendingTree to protect their Personal Information when they provided it as a condition of purchase.

617. LendingTree owed a common law duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Personal Information in its possession from being compromised, accessed, stolen, or misused by unauthorized parties.

618. LendingTree owed a duty to Plaintiffs and Class Members to supervise Snowflake in the collection, storage, and security of Plaintiffs' and Class Members' Personal Information.

619. LendingTree's duty of reasonable care is established by governmental regulations and industry guidance establishing industry standards for data security to safeguard Personal Information stored on cloud platforms, as described herein.

620. LendingTree owed a statutorily imposed duty to Plaintiffs and Class Members to refrain from unfair and deceptive practices.

621. LendingTree understood that it owed a duty of care to Plaintiffs and Class Members to keep their information safe and secure; they acknowledged that data breaches could cause substantial harm to individuals and were foreseeable.

Shortly before the Breach, on February 29, 2024, in its SEC Annual Report, LendingTree explicitly identified data security as a risk facing the business, and stated as follows[197]:

> In the processing of consumer transactions, our businesses collect, use, store, disclose, transfer, and otherwise process a large volume of personal information and other confidential, proprietary and sensitive data. Breaches or failures of security involving our systems or website or those of any of our affiliates, Network Partners or external service providers have occurred in the past and may occur in the future, and have in the past resulted in, and could in the future result in, the theft, unauthorized access, acquisition, use, disclosure, modification or misappropriation of personal information of our consumers, employees or third parties with whom we conduct business, or other confidential, proprietary and sensitive data, fraudulent activity, or system disruptions or shutdowns.
>
> …
>
> [W]e may be held responsible for any breach, failure or fraudulent activity attributed to our affiliates, Network Partners or external service providers as they relate to the information we share with them. In addition, because we do not control our Network Partners or external service providers and our ability to monitor their data security is limited, we cannot ensure the security measures they take will be sufficient to protect our information.

622. Consumers, including the LendingTree Plaintiffs, relied upon or would be reasonable in relying upon LendingTree's express and implied commitments to protect the privacy of their Personal Information when they decided to utilize LendingTree's services.

---

[197] LendingTree, Inc. Form 10-K at 18-19 (Feb. 29, 2024), https://investors.lendingtree.com/node/20321/html.

623. LendingTree knew or should have known of the importance of oversight related to third-party providers. LendingTree has announced compromised consumer data in two prior data breach incidents, in 2008 and 2022.[198] This Data Breach was foreseeable because LendingTree has dealt with data breaches in the past.

III. The LendingTree Defendants breached their duty to protect Personal Information and engaged in unfair trade practices.

624. At the time of the Data Breach, LendingTree failed to maintain reasonable data security measures and comply with FTC guidance and other relevant industry standards summarized herein. These data security failings included:

- LendingTree did not enforce MFA for its Snowflake accounts. Indeed, QuoteWizard chose to use Snowflake to store the Personal Information of millions of its customers despite knowing that Snowflake did not allow customers to enforce MFA.
- LendingTree did not rotate or disable the credentials of old Snowflake accounts.
- LendingTree did not implement network allow lists that Snowflake account access to certain locations or trusted users.

[198] Alex Lekander, *Hacker Leaks Database Claiming to be from LendingTree*, CyberInsider (June 21, 2022), https://cyberinsider.com/lendingtree-data-breach-2022/.

625. LendingTree further failed to properly investigate, retain, oversee and audit a competent cloud-based data storage provider, because Snowflake similarly had numerous data security failings, as described herein.

626. LendingTree's data security failings enabled the Data Breach. Without these basic protections, UNC5537 was able to exfiltrate the Personal Information of over 190 million LendingTree consumers with nothing more than stolen Snowflake credentials obtained through malware campaigns—and traffic the data to other cybercriminals.

627. LendingTree's failings were particularly egregious given the enormous amount of Personal Information it stored on Snowflake's servers. Tasked with handling the data of over 190 million consumers, LendingTree's failure to implement these basic data security measures is all the more inexplicable and reckless.

628. Indeed, each of these basic protections could have prevented the Data Breach. For example:

- Had LendingTree implemented MFA, UNC5537 would not have been able to access QuoteWizard data with just stolen credentials. MFA would have required an additional layer of authentication (i.e., a code sent via text message or email) that UNC5537 would not have had access to.

- LendingTree could have also prevented the Data Breach by maintaining a policy of rotating or disabling credentials that were either old or compromised in other data breaches. As the Mandiant Report found that the "majority of credentials used by

UNC5537" were available from historic malware campaigns dating back to 2020, a policy that disabled previously-compromised credentials could have prevented the Data Breach.[199]

- LendingTree could have also prevented the Data Breach by maintaining stricter network allow lists that restricted access to customer Personal Information to certain locations or trusted user accounts that were not previously compromised.

629. In addition, LendingTree violated the FTC Response Guidance by failing to give affected consumers sufficient information regarding the scale of the attack and the types of information taken in the Notice that consumers were ultimately provided.

630. LendingTree, through these basic data security failings, breached its express representations in its Privacy Policy and Security Policy. These representations included, but are not limited to, statements that LendingTree had implemented measures to "monitor and maintain the security of our systems and networks and to detect, prevent, investigate, and protect you, our business, and others from fraud, unauthorized transactions, and other unlawful or unsafe activity"[200] and that QuoteWizard and LendingTree were "committed to

[199] https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion

[200] QuoteWizard, *Privacy Policy*, *supra* n. 189.

maintaining [consumers'] confidence and trust as it relates to the privacy and security of [consumers'] personal information."[201]

631. In the alternative, LendingTree breached implied commitments to consumers to protect their Personal Information, including the LendingTree Plaintiffs, by virtue of mandating that consumers provide their sensitive Personal Information as a condition of purchase.

632. LendingTree's basic data security failings also breached its duty of care to protect the Personal Information of consumers, which include the LendingTree Plaintiffs.

IV. Personal Information stolen about LendingTree Customers.

633. In late July 2024, LendingTree provided consumers affected by the Data Breach with a Notice that disclosed, "[W]e concluded that the [Data Breach] incident likely resulted in the unauthorized access to our disclosure of consumers' names, residential addresses, and driver's license numbers."[202] The Notice was provided on letterhead that read, "QuoteWizard by LendingTree," instructed consumers to "remain vigilant by reviewing account statements and monitoring

---

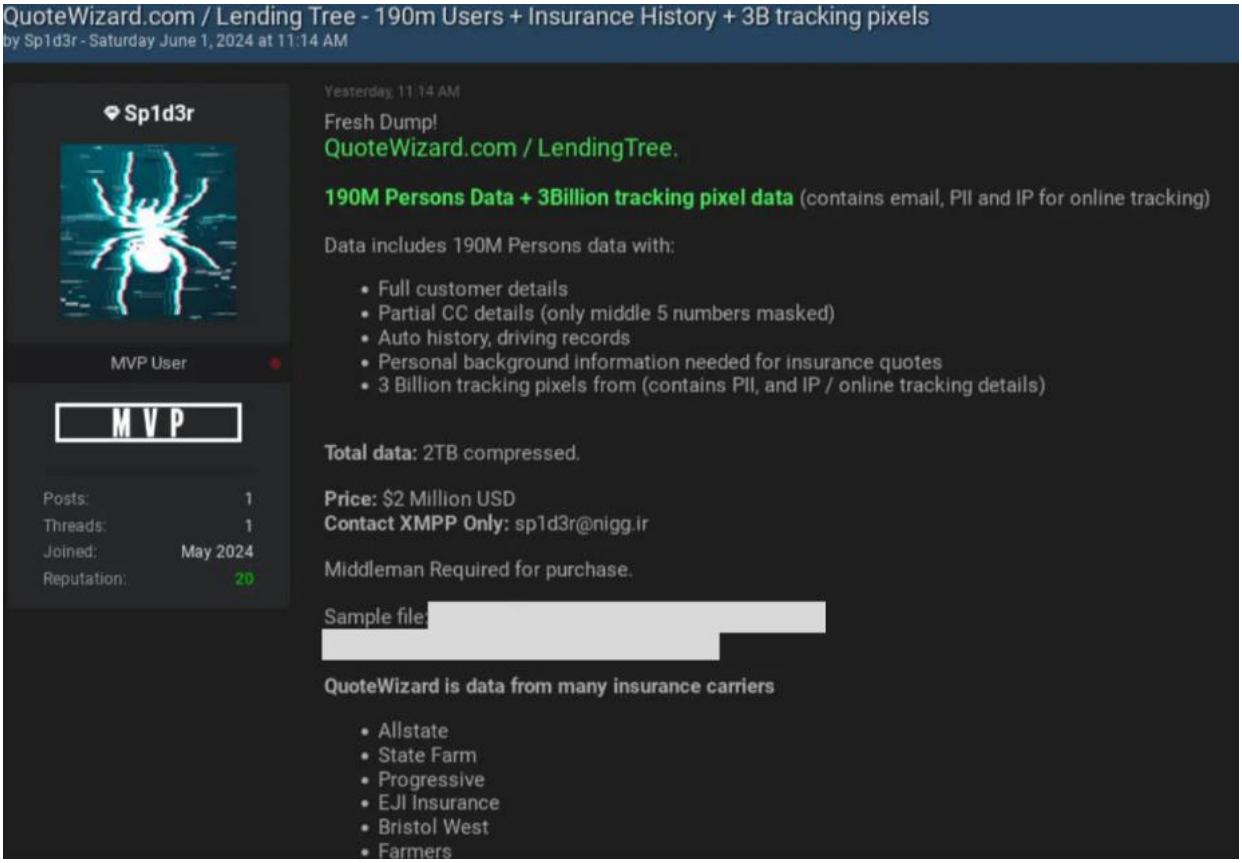
201 *Id.*

202 *Notice of Data Incident*, QuoteWizard by LendingTree (July 30, 2024), https://ago.vermont.gov/sites/ago/files/documents/2024-08-09%20QuoteWizard%20Data%20Breach%20Notice%20to%20Consumers.pdf.

credit reports," and encouraged consumers to enroll in free credit monitoring services provided by LendingTree.

634. The stolen Personal Information also included partial credit card numbers, automobile history, driving records, personal background information needed for insurance quotes, and tracking pixel data related to consumers' internet activity. On June 1, 2024, around the time of the Data Breach, this very information was advertised for sale on a dark web forum post by a cybercriminal group by the name of "Sp1d3r." A screenshot of this post is provided below.[203]

[203] Ashish Khaitan, *Dark Web Actor Claims to Pilfer 2TB of Compressed Data from QuoteWizard*, The Cyber Express (June 3, 2024), https://thecyberexpress.com/alleged-quotewizard-data-breach-claims/; *see also* Matt Burgess, *The Snowflake Attack May Be Turning Into One of the Largest Data Breaches Ever*, Wired (June 6, 2024), https://www.wired.com/story/snowflake-breach-advanced-auto-parts-lendingtree/ (reporting that Sp1d3r claimed data posted on dark web forum was "related to the Snowflake incident").



635. Plaintiffs and Class Members have a privacy interest in the non-disclosure of their driver's license numbers, as they are a static identifier that can be used to perpetrate identity fraud. This is especially the case where, as here, a driver's license number is disclosed alongside other identifiers, including names, addresses, driving records, and tracking pixel data.

V. Plaintiffs and Class Members suffered injuries as a result of the Data Breach.

636. As described herein, the Personal Information exposed in the Data Breach caused injury to LendingTree Plaintiffs and Class Members.

637. First, the Data Breach subjected LendingTree Plaintiffs and Class Members to a substantial risk of identity theft, which is demonstrated by facts including, but not limited to: incidences of identity fraud suffered by the Plaintiffs; the posting of LendingTree Plaintiffs' and Class Members' Personal Information on the dark web; the inadequate vagueness of LendingTree's Notice as to Personal Information taken when compared against the specificity of Personal Information advertised for sale on the dark web; the sensitivity of Personal Information related to payment card data and driver's license numbers; and LendingTree's own Notice that expressly instructed affected customers to "remain vigilant by reviewing account statements and monitoring credit reports" and recommending that customers register for credit monitoring services. As a result of this substantial risk they face, LendingTree Plaintiffs and Class Members reasonably suffered injury in the form of lost time and resources mitigating against the risk of identity theft and emotional distress arising from the risk of identity theft.

638. Second, LendingTree made specific data security representations to LendingTree Plaintiffs and Class Members in the course of soliciting Personal Information to provide insurance quotes. By exposing Personal Information to unauthorized third parties in a manner inconsistent with these representations, LendingTree Plaintiffs and Class Members did not receive the benefit of their

bargain when they provided their Personal Information in exchange for insurance quotes.

639. Third, Personal Information has inherent value, and the exposure of that information makes consumers susceptible to fraud and scams for years into the future. Not only should consumers be compensated for the value of their Personal Information, but they should also be provided with monitoring services to ensure that their data is not misused in the future.

640. Fourth, the disclosure of LendingTree Plaintiffs' and Class Members' private and sensitive nature of the Personal Information to cybercriminals who in turn advertised and sold the Personal Information on the dark web, constitutes a privacy injury.

VI. Class action allegations as to the LendingTree Defendants.

641. The LendingTree Plaintiffs brings this action on their own behalf, and on behalf the following LendingTree Class and Subclasses (the "LendingTree Classes").

- **Nationwide LendingTree Class.** All individuals residing in the United States who QuoteWizard and/or LendingTree identified as being among those individuals whose Personal Information was compromised in the Data Breach (the "LendingTree Class").
- **State-Specific Subclasses.** As described in this Section below, all individuals residing in a specific state who QuoteWizard and/or LendingTree identified as being among those individuals whose Personal Information was compromised in the Data Breach ("LendingTree Subclass").

642. Excluded from the LendingTree Classes are the LendingTree Defendants' officers and directors, any entity in which the LendingTree Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of the LendingTree Defendants. Excluded also from the LendingTree Classes are members of the judiciary to whom this case is assigned, their families and members of their staff.

643. The LendingTree Plaintiffs reserve the right to amend or modify the definition of the LendingTree Classes or create additional subclasses as this case progresses.

644. **Numerosity.** The members of the LendingTree Classes are so numerous that joinder of all of them is impracticable. Public reporting presently indicates that over 190 million LendingTree customers were affected by the Data Breach.

645. **Commonality.** There are questions of fact and law common to the LendingTree Classes, which predominate over individualized questions. These common questions of law and fact include, but are not limited to:

- Whether the LendingTree Defendants had a duty to protect the Personal Information of LendingTree Plaintiffs and Class Members.
- Whether the LendingTree Defendants breached express or implied commitments to protect the Personal Information of LendingTree Plaintiffs and Class Members.

- Whether the LendingTree Defendants knew or should have known that their data security practices were deficient.
- Whether the LendingTree Defendants knew or should have known that their vendor's data security practices were deficient.
- Whether the LendingTree Defendants' data security systems were consistent with industry standards prior to the Data Breach.
- Whether the LendingTree Defendants adequately disclosed details regarding the Data Breach to affected consumers.
- Whether LendingTree Plaintiffs and Class Members are entitled to actual damages, punitive damages, treble damages, statutory damages, general damages, nominal damages, and/or injunctive relief.

646. **Typicality.** The LendingTree Plaintiffs' claims are typical of those of other Class Members because the LendingTree Plaintiffs' Personal Information, like that of every other Class Member, was compromised in the Data Breach

647. **Adequacy of Representation.** The LendingTree Plaintiffs will fairly and adequately represent and protect the interest of the LendingTree Class Members. Plaintiffs' Counsel are competent and experienced in litigating class actions.

648. **Predominance.** The LendingTree Defendants have engaged in a common course of conduct toward the LendingTree Plaintiffs and Class Members, in that all the data of LendingTree Plaintiff and Class Members were stored on the same Snowflake Data Cloud network and unlawfully accessed in the same manner. The common issues arising from the LendingTree Defendants' conduct affecting

Class Members listed above predominate over any individualized issues. Adjudication of these common issues in a single action will advance judicial economy.

649. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of the claims of the LendingTree Classes. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most LendingTree Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual LendingTree Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for QuoteWizard and LendingTree. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each LendingTree Class Member.

650. LendingTree and LendingTree have acted on grounds that apply generally to the LendingTree Class as a whole such that class certification, injunctive relief, and declaratory relief are appropriate on a class-wide basis.

651. Likewise, particular issues are appropriate for certification because such claims present common issues whose resolution would advance the disposition of this matter. Such particular issues include, but are not limited to:

- Whether the LendingTree Defendants owed a legal duty to the LendingTree Plaintiffs and Class Members to protect their Personal Information.
- Whether the LendingTree Defendants' data security measures were inadequate in light of applicable regulations and industry standards.
- Whether the LendingTree Defendants' data security measures were negligent.
- Whether the LendingTree Defendants' oversight over vendors' data security measures was negligent.
- Whether the LendingTree Defendants breached express or implied representations to the LendingTree Plaintiffs and Class Members regarding the protection of their Personal Information.

652. Finally, all members of the proposed LendingTree Classes are readily ascertainable. The LendingTree Defendants have access to the names and contact information of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by QuoteWizard and LendingTree.

VII. Causes of action as to the LendingTree Defendants.

FIRST CLAIM FOR RELIEF
Negligence
On behalf of the LendingTree Plaintiffs and the LendingTree Class

653. The LendingTree Plaintiffs repeat and re-allege the allegations contained in Paragraphs 1 through 150, as well as Part One and Part Five, as set forth fully herein.

654. The LendingTree Defendants owed a duty under common law to the LendingTree Plaintiffs and LendingTree Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, and deleting their Personal Information in its possession from being compromised, stolen, or misused by unauthorized persons.

655. Specifically, this duty included, among other things: (a) implementing industry standard data security safeguards to protect the Personal Information of LendingTree Plaintiffs and LendingTree Class Members such as MFA, rotating credentials, and restricting access privileges; (b) maintaining, testing, and monitoring the LendingTree Defendants' security systems to ensure that Personal Information was adequately secured and protected; (c) overseeing and monitoring vendor Snowflake to ensure adequate standards were in place for the security of consumer Personal information; (d) timely acting upon warnings and alerts to respond to intrusions; and (e) adequately notifying the LendingTree Plaintiffs and Class Members about the types of data that were compromised in the Data Breach.

656. The LendingTree Defendants' duty to use reasonable care in protecting the Personal Information they collected arose from several sources, including those set out below.

657. The LendingTree Defendants had a common law duty to prevent foreseeable harm to others. This duty existed because the LendingTree Defendants collected and stored valuable Personal Information that is routinely targeted by cyber criminals. The LendingTree Plaintiffs and LendingTree Class Members were the foreseeable and probable victims of any compromise to inadequate data security practices maintained by the LendingTree Defendants.

658. The LendingTree Defendants further assumed a duty of reasonable care in promulgating their Privacy and Security Policies which assured the LendingTree Plaintiffs and LendingTree Class Members that their Personal Information would be adequately secured.

659. The LendingTree Defendants breached their duties owed to the LendingTree Plaintiffs and LendingTree Class Members by failing to maintain adequate data security practices that conformed with industry standards, and were therefore negligent.

660. The LendingTree Defendants breached their duties owed to LendingTree Plaintiffs and Class Members by failing to exercise reasonable oversight in the selection of Snowflake to store Personal Information. Such

reasonable oversight would have revealed that Snowflake's cloud services lacked industry standard data security safeguards necessary to adequately protect Personal Information.

661. But for the LendingTree Defendants' negligence, the Personal Information of the LendingTree Plaintiffs and LendingTree Class Members would not have been stolen by cybercriminals in the Data Breach.

662. As a direct and proximate result of the LendingTree Defendants' breach of duties, the LendingTree Plaintiffs and LendingTree Class Members have suffered injuries detailed above.

663. As a direct and proximate result of the LendingTree Defendants' negligence, the LendingTree Plaintiffs and LendingTree Class Members are entitled to damages, including compensatory, general, nominal, and/or punitive damages, in an amount to be proven at trial.

SECOND CLAIM FOR RELIEF
Violation of Washington Consumer Protection Act ("WPCA")
(Wash. Rev. Code An. §§ 19.86.020, et seq.)
On behalf of Plaintiffs Macom, Nader, and N. Thomas and a LendingTree Subclass of Washington Residents

664. Plaintiffs Macom, Nader, and N. Thomas (together, the "Washington Plaintiffs") repeat and re-allege the allegations contained in Paragraphs 1 through 150, as well as Part One and Part Five, as set forth fully herein.

665. The Washington Plaintiffs and Washington LendingTree Subclass Members are "persons" under the WPCA because they are natural persons. Wash. Rev. Code Ann. § 19.86.010(1).

666. The LendingTree Defendants are "persons" under the WPCA because they are corporations. Wash. Rev. Code Ann. § 19.86.010(1).

667. The LendingTree Defendants engaged in "trade" and "commerce" as defined by the WPCA because they provided insurance quote comparison services, which offers the sale of insurance products, to Washington consumers. Wash. Rev. Code Ann. § 19.86.010(2).

668. The LendingTree Defendants engaged in unfair trade practices prohibited by the WPCA. Wash. Rev. Code Ann. § 19.86.020.

669. The LendingTree Defendants engaged in unfair trade practices when they failed to maintain reasonable data security practices to safeguard the Personal Information of the Washington Plaintiffs and Washington LendingTree Subclass Members, including: (a) failing to implement industry standard data security safeguards to protect the Personal Information of Washington Plaintiffs and Washington LendingTree Subclass Members relating to MFA, rotating credentials, and restricting access privileges; (b) failing to maintain, test, and monitor Snowflake's security systems to ensure that Personal Information was adequately

secured and protected; and (c) failing to implement intrusion detection systems and notifying customers of suspicious intrusions.

670. The LendingTree Defendants' conduct offends established public policy and is immoral, unethical, oppressive, unscrupulous and substantially injurious to consumers.

671. The LendingTree Defendants' conduct is injurious to the public interest because it violates Wash. Rev. Code Ann. § 19.86.020 and/or has the capacity to injure persons, including the many Washington consumers affected by the Data Breach.

672. As a direct and proximate result of the LendingTree Defendants' unfair trade practices, the Washington Plaintiffs and Washington LendingTree Subclass members have suffered injuries as described above.

673. The Washington Plaintiffs and Washington Subclass Members thus seek all monetary and non-monetary relief allowed by law, including injunctive relief, damages, including actual damages in an amount to be proven at trial, treble damages of actual damages, and reasonable attorneys' fees.

THIRD CLAIM FOR RELIEF
Unjust Enrichment
On behalf of the LendingTree Plaintiffs and the LendingTree Class

674. The LendingTree Plaintiffs repeat and re-allege the allegations contained in Paragraphs 1 through 150, as well as Part One and Part Five, as set forth fully herein.

675. LendingTree's Product and Privacy Policy states that it may use collected information to communicate products and services that might be of interest to customers and potential customers, create anonymized or aggregated data, or deliver products or services to customize a customer or potential customer's user experience.

676. Further, LendingTree states that it may share information it collects on customers and potential customers with third parties, including affiliates, network and product partners, financial companies, business partners, and others, who use this information for marketing purposes.

677. The information LendingTree gathers is therefore monetized by LendingTree for commercial purposes.

678. LendingTree collected sensitive Personal Information without taking measures to protect that information.

679. LendingTree monetized Personal Information and did not take reasonable data security measures to protect that information.

680. LendingTree was able to gain a commercial advantage and make a profit from Personal Information because it did not invest in reasonable data security to protect that information.

681. It would be unjust for LendingTree to retain the benefit it realized from collecting Personal Information and not investing reasonable time, effort, and resources to protect that information.

682. LendingTree has been unjustly enriched by its collection of Plaintiffs' and Class Members' Personal Information because it did not invest reasonable time, effort, and resources to protect that information.

683. Plaintiffs and Class Members have been injured by LendingTree's unjust enrichment related to the collection of their Personal Information without paying to protect that information. Accordingly, Plaintiffs and Class Members are entitled to damages including, but not limited to, disgorgement.

PART SIX: AT&T DEFENDANTS

684. Plaintiffs Latosha Austin, Gilbert Criswell, Roscoe Eldridge, David Hornthal, Traci Lively, Natasha McIntosh and Debby Worley (collectively, the "AT&T Plaintiffs") are named in this Representative Complaint to pursue claims against AT&T.[204]

I. The AT&T Defendants' business and data security promises.

685. AT&T "provides more than 100 million U.S. consumers with communications experiences across mobile and broadband."[205]

686. AT&T admits that it has a "duty under federal law to protect the confidentiality of" the call records information AT&T collects, including Personal Information.[206] This is true: 47 U.S.C. § 222 (Privacy of customer information) imposes a duty on AT&T to protect the confidentiality of customer proprietary network information and is prohibited from disclosure, except as required by law or with the customer's permission.

---

[204] AT&T, Inc. and AT&T Mobility, LLC are collectively referred to herein as "AT&T" or the "AT&T Defendants" except as expressly delineated.

[205] AT&T, Investor Profile, https://investors.att.com/investor-profile (last visited Aug. 19, 2024).

[206] AT&T Privacy Notice (effective date December 11, 2023 through July 16, 2024), https://web.archive.org/web/20231212012645/https://about.att.com/privacy/privacy-notice.html.

687. AT&T claims it maintains "a network and information security program that is reasonably designed to protect our information, and that of our customers, from unauthorized risks to their confidentiality, integrity, or availability."[207]

688. When disclosing the Data Breach, AT&T reaffirmed its promises that: "We hold ourselves to a high standard and commit to delivering the experience that you deserve. We constantly evaluate and enhance our security to address changing cybersecurity threats and work to create a secure environment for you. We invest in our network's security using a broad array of resources including people, capital, and innovative technology advancements."[208]

689. AT&T owed a duty of care to Plaintiffs and Class Members. As a condition of providing telecommunication services, including allowing its customers to call and text non-AT&T customers, and allowing non-AT&T customers to call and text AT&T customers, AT&T collected, stored, shared, and maintained Plaintiffs' and Class Members' Personal Information, including on the Snowflake cloud-based data storage systems involved in the Data Breach.

---

[207] AT&T Inc., 2023 Annual Report, https://investors.att.com/financial-reports/annual-reports/2023 (last visited Aug. 20, 2024).

[208] *Unlawful access of customer data*, AT&T (July 24, 2024), https://www.att.com/support/article/myaccount/000102979?source=EPcc000000000000U (last visited Aug. 19, 2024).

690. AT&T shared Plaintiffs' and Class members' Personal Information with Snowflake in the course of using services provided by Snowflake.

691. AT&T, in collecting such sensitive Personal Information from consumers, owed a duty of care to consumers, including the AT&T Plaintiffs, to exercise reasonable care in maintaining, protecting, and securing their Personal Information. AT&T**,** by mandating the collection of sensitive Personal Information from consumers as a condition of purchasing goods and services, implied its assent to consumers to protect their Personal Information. Consumers expected AT&T to protect their Personal Information when they provided it as a condition to procure goods and services**.** AT&T owed a common law duty to the AT&T Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Personal Information in Snowflake's possession from being compromised, accessed, stolen, or misused by unauthorized parties.

692. AT&T owed a common law duty to Plaintiffs and Class Members to supervise Snowflake in the collection, storage, and security of the AT&T Plaintiffs' and Class Members' Personal Information.

693. AT&T's duty of reasonable care is established by federal statute, governmental regulations and industry guidance establishing industry standards for

data security to safeguard Personal Information stored on cloud platforms, as described herein.

694. AT&T also owed a statutorily imposed duty to the AT&T Plaintiffs and Class Members to refrain from unfair and deceptive practices.

695. AT&T owed a statutorily imposed duty, pursuant to 47 U.S.C § 222, to safeguard customer information against unauthorized disclosure—such as the Data Breach.

696. AT&T knew of the importance of implementing basic cybersecurity, as well as exercising oversight over third-party providers for a number of reasons.

697. First, AT&T is credited as having invented MFA three decades ago, holding a patent for a "transaction authorization and alert system" that allowed customers to authorize transactions through the use of a messaging or alert system.[209]

698. Second, AT&T advertises MFA products to its business clients for purchase, noting that using MFA could stave off data breaches. "The majority of data breaches are caused by brute force attacks on credentials. . . . AT&T Multi-

[209] AT&T Corp., Transaction authorization and alert system, P0745961 (A2), https://worldwide.espacenet.com/publicationDetails/biblio?DB=worldwide.espacenet.com&II=0&ND=3&adjacent=true&locale=en_EP&FT=D&date=19961204&CC=EP&NR=0745961A2&KC=A2; Jon Brodkin, *Kim Dotcom claims he invented two-factor authentication—but he wasn't the first*, ArsTechnica (May 23, 2013), https://arstechnica.com/information-technology/2013/05/kim-dotcom-claims-he-invented-two-factor-authentication-but-he-wasnt-first/.

Factor Authenticator (AT&T MFA) uses next generation security protocols available to protect your network and devices from breaches related to identity. Cybercriminals use automated code breaking brute force attacks to infiltrate a network, steal passwords, and steal or ransom your data or your customers' data. It's more difficult and costly to clean up after an attack than to prevent it in the first place. To stay ahead on security, it's a smart move to invest in a virtually unphishable credential authentication system."[210]

699. Third, AT&T has suffered a number of data breaches, demonstrating to the company that a failure to implement and follow cybersecurity guidelines can result in the exposure of customer data.[211]

700. The Data Breach is the second breach of AT&T customer data last year. Earlier last year, data of over 70 million AT&T customers—including encrypted passcodes for accessing AT&T customer accounts—was published on a cybercrime forum. AT&T confirmed the data was authentic, but does not know whether the data originated from AT&T or one of its vendors.[212] The breached data

---

[210] *Secure access to your corporate network and prevent identity fraud with AT&T Multi-Factor Authenticator* (2022), https://cdn-cybersecurity.att.com/docs/product-briefs/att-multi-factor-authenticator.pdf.

[211] Catherine Reed, *AT&T Data Breaches: Full Timeline Through 2023*, Firewall Times (Oct. 5, 2023), https://firewalltimes.com/att-data-breaches/.

[212] Becky Bracken, *AT&T Confirms 73M Customers Affected in Data Leak*, DarkReading (Apr. 1, 2024), https://www.darkreading.com/remote-workforce/att-

includes names, phone numbers, postal addresses, and Social Security numbers.[213] Based on AT&T's preliminary analysis, the data appears to be from 2019 or earlier, impacting approximately 7.6 million current AT&T account holders and approximately 65.4 million former account holders.[214] AT&T claims there is no evidence this was the result of unauthorized access to its systems.[215]

701. In the last ten years, AT&T was also the subject of several additional data breaches involving customer data in 2014, 2020, 2022, and 2023.[216]

702. A company with such extensive experience in prior breaches should understand and appreciate the significant risk of harm that breaches expose customers to. AT&T knew or was reckless in not knowing that substandard data security practices or ineffective monitoring of third-party providers could—and often do—lead to data breaches.

---

confirms-73m-customers-affected-data-leak; AT&T Inc., *AT&T Addresses Recent Data Set Released on the Dark Web* (Mar. 30, 2024), https://about.att.com/story/2024/addressing-data-set-released-on-dark-web.html (last visited Aug. 20, 2024).

213 *Id*.

214 *Id*.

215 *Id*.

216 Catherine Reed, *AT&T Data Breaches: Full Timeline Through 2023*, Firewall Times (Oct. 5, 2023), https://firewalltimes.com/att-data-breaches/ (last visited Aug. 20, 2024).

703. This Data Breach was foreseeable because AT&T has dealt with data breaches involving third-party vendors in the past.

II. The AT&T Defendants breached their duty to protect Personal Information and engaged in unfair trade practices.

704. Despite AT&T's explicit assurances that it would safeguard its customers' sensitive Personal Information, AT&T notified customers that customer information was "illegally downloaded" from their Snowflake cloud platforms.

705. Information exposed in the Data Breach not only consisted of sensitive call logs for AT&T consumers, but it also disclosed with whom those customers interacted (regardless of service provider), call logs for individuals whose numbers are on customer accounts, and former customers.

706. The Data Breach accordingly exposed the Personal Information of nearly every person in the United States with a cell phone number.

707. The compromised information is uniquely sensitive. For example, cell site identification numbers can be used to determine the approximate location of where a call was made or text message sent. Cybercriminals can also now identify relationships among phone numbers, allowing hackers to make scams more believable. With the compromised Personal Information, hackers can determine which banks, medical providers, schools, charities, stores, and other individuals a person is in contact with, further expanding the range and effectiveness of phishing

and other attempts to trick impacted individuals into giving up yet more personal or financial information.[217]

708. AT&T's announcements of the Data Breach did not include a critical piece of information: hackers could not have "illegally downloaded" information about customers had AT&T deployed basic cybersecurity measures to protect their Snowflake accounts.

709. Additionally shocking is that, although AT&T learned of the Data Breach on April 19, 2024, hackers were still able to continue exfiltrating data on their customers until April 25, 2024.[218]

710. At the time of the Data Breach, AT&T failed to maintain reasonable data security measures and comply with FTC guidance, the PCI DSS, and other relevant industry standards summarized above. These data security failings included:

- AT&T did not enforce MFA for its Snowflake accounts.
- AT&T did not rotate or disable the credentials of old Snowflake accounts.

---

[217] Ramishah Maruf, *How AT&T customers can protect themselves in the latest data breach*, CNN (July 12, 2024), https://www.cnn.com/2024/07/12/business/att-customers-data-breach-protection/index.html.

[218] Lily Hay Newman, *The Sweeping Danger of the AT&T Phone Records Breach*, Wired (Jul. 12, 2024), https://www.wired.com/story/att-phone-records-breach-110-million/.

- AT&T did not implement network allow lists that restricted Snowflake account access to certain locations or trusted users.

711. AT&T failed to take these measures despite being under constant attacks and attempted attacks from threat actors.

712. AT&T's data security failings enabled the Data Breach. Without these basic protections, UNC5537 was able to exfiltrate the Personal Information of millions of consumers with nothing more than stolen AT&T or Snowflake credentials.

713. Indeed, each of these basic protections could have prevented the Data Breach. For example:

- Had AT&T implemented MFA, UNC5537 would not have been able to access AT&T data with stolen or outdated credentials. MFA would have required an additional layer of authentication (i.e., a code sent via text message or email) that UNC5537 would not have had access to.

- AT&T could have also prevented the Data Breach by maintaining a policy of rotating or disabling credentials that were either old or compromised in other data breaches. As the Mandiant Report found that a "majority of the credentials used by UNC5537" were available from historic malware campaigns dating back to 2020, a policy that disabled previously-compromised credentials could have prevented the Data Breach.[219]

- AT&T could have also prevented the Data Breach by maintaining stricter network allow lists that restricted access to

[219] The Mandiant Report, *supra* n. 24.

> customer Personal Information to certain locations or trusted user accounts that were not previously compromised.

714. AT&T, through these basic data security failings, breached express representations to consumers regarding protecting Personal Information and implementing cybersecurity policies. In the alternative, AT&T breached implied commitments to protect consumer Personal Information made to consumers by virtue of having access to some of the most sensitive data available to hackers and opting to simply not protect it.

715. AT&T's basic data security failings also breached its duty of care to protect the Personal Information of consumers.

III. Personal Information stolen about AT&T Plaintiffs and Class Members.

716. In a July 12, 2024 press release, AT&T acknowledged that "customer data was illegally downloaded from our workspace on a third-party cloud platform." The press release, excerpted at greater length below, disclosed that the stolen data included "AT&T records of calls and texts of nearly all of AT&T's cellular customers . . . between May 1, 2022 – October 31, 2022" and also included for a subset of stolen records, "one or more cell site identification number(s) associated with the [telecommunications] interaction."[220]

> Based on our investigation, the compromised data includes files containing **AT&T records of calls and texts of nearly all of AT&T's**

[220] *AT&T Addresses Illegal Download of Customer Data*, AT&T (July 12, 2024), https://about.att.com/story/2024/addressing-illegal-download.html.

> **cellular customers**, customers of mobile virtual network operators (MVNOs) using AT&T's wireless network, as well as AT&T's landline customers who interacted with those cellular numbers between May 1, 2022 - October 31, 2022. The compromised data also includes records from January 2, 2023, for a very small number of customers. The records identify the telephone numbers an AT&T or MVNO cellular number interacted with during these periods. For a subset of records, one or more cell site identification number(s) associated with the interactions are also included.

717. The scale of this breach is enormous. Based on AT&T's annual report of its total customers in 2022 and its disclosure that "nearly all" were affected, the Data Breach impacted over 100 million customers.[221]

718. An individual's call and text logs are private and sensitive information. Indeed, Congress made these precise findings when it passed the Telephone Records and Privacy Protection Act of 2006 ("TRPPA"), which criminalized the unauthorized disclosure of phone records.[222] In passing the TRPPA, Congress made express findings that "telephone records can be of great use to criminals because the information contained in call logs may include a wealth of personal data"; that "call logs may reveal the names of telephone users' doctors, public and private relationships, business associates, and more" and that "the unauthorized disclosure

---

221 Matt Kapko, *Massive Snowflake-linked attack exposes data on nearly 110M AT&T customers*, Cybersecurity Dive (July 12, 2024), https://www.cybersecuritydive.com/news/att-cyberattack-snowflake-environment/721235/.

222 Telephone Records and Privacy Protection Act of 2006, 18 U.S.C. § 1039.

of telephone records not only assaults individual privacy but, in some instances, may further acts of domestic violence or stalking, compromise the personal safety of law enforcement officers, their families, victims of crime, witnesses, or confidential informants, and undermine the integrity of law enforcement investigations."[223]

719. Further demonstrating how an individual's call logs can disclose private relationships and connections, after the Data Breach, FBI officials warned its agents that their call logs were presumed stolen and that the identity of confidential informants could be compromised. The FBI urged agents to take action to limit the fallout given the possibility of hackers publicly disclosing the stolen call logs.[224]

720. Industry experts have highlighted additional serious privacy and fraud concerns associated with the theft of call logs and cell cite identification numbers:

> There are many effects of this breach. If someone gets their hands on this much info, they could use it in a lot of bad ways. This information could be used by cybercriminals to target phishing attacks, steal your name, or even demand money. Cybercriminals can make more effective phishing schemes if they know specific details about people, like their phone numbers and how often they call. The data could also be used to

---

223 18 U.S.C. § 1039, Notes 1-2, 5.

224 Jake Bleiberg and Margi Murphy, *FBI Warned Agents It Believes Phone Logs Hacked Last Year*, Bloomberg (Jan. 16, 2025), https://www.bloomberg.com/news/articles/2025-01-16/fbi-has-warned-agents-it-believes-hackers-stole-their-call-logs/.

> figure out personal things about people, like their relationships, health, or finances, which could then be used for bad things.[225]

721. Security experts warn that the information can expose consumers to significant harm and fraud.

> "Yeah, this is really bad," says Jake Williams, vice president of research and development at the cybersecurity consultancy Hunter Strategy. "What the threat actors stole here are essentially call data records. These are a gold mine in intelligence analysis because they allow someone to understand networks—who is talking to whom and when. And threat actors have data from previous compromises to map phone numbers to identities. But even without identifying data for a phone number, closed networks—where numbers *only* communicate with others in the same network—are almost always interesting."[226]

722. Contrary to guidance from the FBI, AT&T paid a hacker approximately $370,000 to delete the data.[227] But that payment does not guarantee that the information was destroyed. Indeed, the phone record data stolen from the breach has sprung up for sale in other forums, demonstrating that the information was likely transferred to other threat actors before it was "deleted."

---

225 Elena Thomas, *Exposed in Massive Cyber Attack*, Cyber Defense Magazine (Jan. 8, 2025), https://www.cyberdefensemagazine.com/att-breach-2024-customer-data-exposed-in-massive-cyber-attack/.

226 Lily Hay Newman, *The Sweeping Danger of the AT&T Phone Records Breach*, Wired (Jul. 12, 2024), https://www.wired.com/story/att-phone-records-breach-110-million/.

227 *AT&T Data Breach: Nearly ALL Customers Have Phone Records Stolen*, Trend (Jul. 15, 2024), https://news.trendmicro.com/2024/07/15/att-data-breach-110-million/.

723. A former counterintelligence officer for the FBI seems to have no confidence that the data stolen was actually deleted, either:

> Darren Mott, who oversaw counterintelligence investigations in the FBI's Huntsville, Alabama, office, said the bureau and other law enforcement and intelligence agencies have likely moved to protect sources based on the assumption that this data will eventually get out.[228]

724. AT&T's conduct has created a substantial risk of identity theft, fraud, or other forms of exploitation. The data acquired in the Data Breach included unencrypted phone numbers and cell site identification numbers, which can be used to perpetuate fraud, identity theft, and other types of exploitation. For example, this data can be used in SIM swapping scams, port-out fraud,[229] and Smishing attacks.[230]

725. Telephone numbers also carry a "treasure trove of information that can be harnessed for various purposes."[231] Even "imprecise and sparse telephone metadata" could allow a cybercriminal to infer a person's home location.[232]

---

228 Jake Bleiberg and Margi Murphy, *FBI Warned Agents It Believes Phone Logs Hacked Last Year*, Bloomberg (Jan. 16, 2025), https://uk.news.yahoo.com/fbi-warned-agents-believes-hackers-185420839.html.

229 Andrew Regitsky, *FCC Will Update CPNI Rules to Stop Data Breaches*, CCMI, https://www.ccmi.com/fcc-will-update-cpni-rules-to-stop-data-breaches/ (last visited Aug. 20, 2024).

230 Fed. Commc'n Comm., Avoid the Temptation of Smishing Scams (Feb. 1, 2024), https://www.fcc.gov/avoid-temptation-smishing-scams (last visited Aug. 20, 2024).

231 Jonathan Mayer et al., *Evaluating the privacy properties of telephone metadata*, 113 PNAS 5536, 5538 (2016).

232 *Id*.

726. While the Personal Information stolen in the Data Breach does not include customer names, AT&T itself admitted, in disclosing the Data Breach, that "there are often ways, using publicly available online tools, to find the name associated with a specific telephone number."[233] According to Information Security experts, once you have a name, the stolen data can then be used to learn more about people: "who they talk to, where they go, where they socialize" and such information "is a treasure trove for people who ultimately would want to do harm."[234]

727. Telephone numbers, even when anonymized, are "trivially reidentifiable" through methods such as basic web searches.[235]

728. Telephone metadata such as that involved in the Data Breach also enables cybercriminals to determine sensitive traits and characteristics of Plaintiff and Class members, such as potential medical conditions, relationship status, religious affiliation, or firearm ownership.[236]

---

233 AT&T, Form 8-K (July 12, 2024), https://www.sec.gov/ix?doc=/Archives/edgar/data/0000732717/000073271724000046/t-0240506.htm.

234 Hank Sanders, *Are You an AT&T Customer? Here's What to Know About the Data Breach*, New York Times (July 12, 2024), https://www.nytimes.com/2024/07/12/us/phone-data-breach.html/.

235 Jonathan Mayer et al., *Evaluating the privacy properties of telephone metadata*, 113 PNAS 5536, 5538 (2016).

236 *Id*. at 5539-40.

729. The potential exposure of this information is particularly alarming, according to Secure Cyber Defense CEO Shawn Waldman, because this type of data allows hackers to pinpoint locations based on phone numbers.[237] Jake Williams, a former hacker for the National Security Agency, said call data records "are a gold mine in intelligence analysis because they can be used to understand who is talking to who—and when."[238] This type of information can be used to craft highly sophisticated attacks through phishing or hacking.[239]

730. The potential for triangulation of customers' locations from compromised cell site identification numbers further "adds a physical dimension to the already extensive privacy violation and could expose individuals to highly targeted and convincing social engineering attacks, not to mention compromising [their] physical security…."[240]

---

237 Stephanie Schappert, *AT&T reports arrest made in April hack, updates affected customers*, cybernews (July 18, 2024), https://cybernews.com/news/att-breach-hack-reports-arrest-made/ (last visited Aug. 20, 2024).

238 Lily H. Newman, *The Sweeping Danger of the AT&T Phone Records Breach*, WIRED, https://www.wired.com/story/att-phone-records-breach-110-million/ (last visited Aug. 20, 2024).

239 Hank Sanders, *Are You an AT&T Customer? Here's What to Know About the Data Breach*, New York Times (July 12, 2024), https://www.nytimes.com/2024/07/12/us/phone-data-breach.html#:~:text=In%20addition%20to%20the%20personal,through%20phishing%20or%20hacking%2C%20Mr.

240 Nate Nelson, *AT&T Breach May Also Impact Millions of Boost, Cricket, H2O Customers*, DarkReading (July 12, 2024),

731. Thus, even without contents of communications, the compromised metadata has "major implications for people's privacy and security."[241]

732. Exacerbating the risk of identity theft to Plaintiffs and Class Members, cybercriminals connected with the Data Breach have advertised and sold the stolen Personal Information on dark web forums.[242]

IV. Plaintiffs and Class Members suffered injuries as a result of the Data Breach.

733. As described herein, the Personal Information exposed in the Data Breach caused injury to Plaintiffs and Class Members.

734. First, the Data Breach subjected Plaintiffs and Class Members to a substantial risk of identity theft as demonstrated by facts including, but not limited to: incidences of identity fraud suffered by the AT&T Plaintiffs; the posting of AT&T Plaintiffs' and Class Members' Personal Information on the dark web; the sensitivity of Personal Information related to call log and location data; and AT&T's own Notice that directs customers to a website called CyberAware for

---

https://www.darkreading.com/cyberattacks-data-breaches/att-breach-may-also-impact-millions-of-boost-cricket-h2o-customers (last visited Aug. 21, 2024).

241 Lily H. Newman, *The Sweeping Danger of the AT&T Phone Records Breach*, WIRED, https://www.wired.com/story/att-phone-records-breach-110-million/ (last visited Aug. 20, 2024).

242 Jessica Lyons, *US Army soldier who allegedly stole Trump's AT&T call logs arrested*, The Register (Jan. 1, 2025), https://www.msn.com/en-us/news/crime/us-army-soldier-who-allegedly-stole-trumps-at-t-call-logs-arrested/ar-AA1wNlhv.

customers to "[f]ind more tips and info" about how to protect themselves after the Data Breach, which includes tutorials for customers to protect against identity theft, phishing, and other fraudulent schemes.[243] As a result of this substantial risk, AT&T Plaintiffs and Class Members reasonably suffered injury in the form of lost time and resources mitigating against the risk of identity theft and emotional distress arising from the risk of identity theft.

735. Second, AT&T made specific data security representations to AT&T Plaintiffs and Class Members. A portion of the price that AT&T Plaintiffs and Class Members pay to AT&T would cover cybersecurity and protection of Personal Information. By exposing Personal Information to unauthorized third parties, Plaintiffs and Class Members did not receive the benefit of their bargain.

736. Third, Personal Information has inherent value, and the exposure of that information makes consumers susceptible to fraud and scams for years into the future. Not only should consumers be compensated for the value of their Personal Information, but they should also be provided with monitoring services to ensure that their data is not misused in the future.

---

[243] *Unlawful access of customer data*, AT&T, https://www.att.com/support/article/my-account/000102979?source=EPcc000000000000U; *CyberAware*, https://about.att.com/pages/cyberaware (last accessed Jan. 17, 2025).

737. Fourth, the disclosure of AT&T Plaintiffs' and Class Members' private and sensitive Personal Information to cybercriminals, who in turn advertised and sold that Personal Information on the dark web, constitutes a privacy injury.

V. Class action allegations as to the AT&T Defendants.

738. The AT&T Plaintiffs bring this action on their own behalf, and on behalf the following AT&T Class and Subclasses (the "AT&T Classes").

- **Nationwide AT&T Class.** All individuals residing in the United States who AT&T identified as being among those individuals whose Personal Information was compromised in the Data Breach (the "AT&T Class").
- **Nationwide Cricket Wireless Class.** All individuals residing in the United States who Cricket Wireless identified as being among those individuals whose Personal Information was compromised in the Data Breach (the "Cricket Wireless Class").
- **Nationwide Non-Customer AT&T Class.** All individuals residing in the United States who either: (a) have been identified as being among those individuals whose Personal Information was compromised in the Data Breach by a mobile virtual network operator ("MVNO") not affiliated with AT&T, including but not limited to Consumer Cellular and Boost Mobile; or (b) exchanged communications with a customer of AT&T, Cricket Wireless, or AT&T's MVNOs between May 1, 2022, and October 21, 2022. Excluded from this Class are current AT&T customers (the "AT&T Non-Customer Class").
- **State-Specific Subclasses.** As described in this Section below, all individuals residing in a specific state who AT&T and/or MVNOs identified as being among those individuals whose Personal Information was compromised in the Data Breach ("AT&T Subclass").

739. Excluded from the AT&T Classes are AT&T and impacted MVNO officers and directors, any entity in which AT&T or impacted MVNOs have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of AT&T or impacted MVNOs. Excluded also from the AT&T Classes are members of the judiciary to whom this case is assigned, their families and members of their staff.

740. The AT&T Plaintiffs reserve the right to amend or modify the definition of the AT&T Classes or create additional subclasses as this case progresses.

741. **Numerosity.** The members of the AT&T Classes are so numerous that joinder of all of them is impracticable. Public reporting presently indicates that over hundreds of millions of individuals were affected by the Data Breach.

742. **Commonality.** There are questions of fact and law common to the AT&T Classes, which predominate over individualized questions. These common questions of law and fact include, but are not limited to:

- Whether AT&T had a duty to protect the Personal Information of AT&T Plaintiffs and Class Members.
- Whether AT&T breached express or implied commitments to protect the Personal Information of AT&T Plaintiffs and Class Members.
- Whether AT&T knew or should have known that its data security practices were deficient.

- Whether AT&T's data security systems were consistent with industry standards prior to the Data Breach.
- Whether AT&T adequately disclosed details regarding the Data Breach to affected consumers.
- Whether AT&T unlawfully utilized, retained, misplaced, or exposed Plaintiffs' and the Class Members' Personal Information.
- Whether AT&T Plaintiffs and Class Members are entitled to actual damages, punitive damages, treble damages, statutory damages, general damages, nominal damages, and/or injunctive relief.

743. **Typicality.** The AT&T Plaintiffs' claims are typical of those of other Class Members because the AT&T Plaintiffs' Personal Information, like that of every other Class Member, was compromised in the Data Breach

744. **Adequacy of Representation.** The AT&T Plaintiffs will fairly and adequately represent and protect the interest of the AT&T Class Members. Plaintiffs' Counsel are competent and experienced in litigating class actions.

745. **Predominance.** AT&T has engaged in a common course of conduct toward the AT&T Plaintiffs and Class Members, in that all the data of Plaintiff and Class Members were stored on the same Snowflake Data Cloud network and unlawfully accessed in the same manner. The common issues arising from AT&T's conduct affecting Class Members listed above predominate over any individualized issues. Adjudication of these common issues in a single action will advance judicial economy.

746. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of the claims of the AT&T Classes. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most AT&T Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual AT&T Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for AT&T. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each AT&T Class Member.

747. **Injunctive Relief.** AT&T has acted on grounds that apply generally to the AT&T Class as a whole such that class certification, injunctive relief, and declaratory relief are appropriate on a class-wide basis.

748. **Issue Certification.** Likewise, particular issues are appropriate for certification because such claims present common issues whose resolution would advance the disposition of this matter. Such particular issues include, but are not limited to:

- Whether AT&T owed a legal duty to the AT&T Plaintiffs and Class Members to protect their Personal Information.

- Whether AT&T's data security measures were inadequate in light of applicable regulations and industry standards.
- Whether AT&T's data security measures were negligent.
- Whether AT&T breached express or implied representations to the AT&T Plaintiffs and Class Members regarding the protection of their Personal Information.

749. **Identification of Class Members Using Objective Criteria.** Finally, all members of the proposed AT&T Classes are readily identifiable using objective criteria. AT&T has access to the names and contact information of Class Members affected by the Data Breach. Adequate notice can be given to Class members directly using information maintained in Defendants' records.

VI. Causes of action against the AT&T Defendants.

FIRST CLAIM FOR RELIEF
Negligence

On behalf of the AT&T Plaintiffs, the Nationwide AT&T Class, the Nationwide Cricket Wireless Class and the Nationwide Non-Customer AT&T Class

750. The AT&T Plaintiffs repeat and re-allege the allegations contained in Paragraphs 1 through 150, as well as Part One and Part Six, as set forth fully herein.

751. The AT&T Defendants owed a duty under common law to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, and deleting their Personal Information in its possession from being compromised, stolen, or misused by unauthorized persons.

752. As described herein, the AT&T Defendants had a duty to: (a) implement industry standard data security safeguards to protect the Personal

Information of AT&T Plaintiffs and Class Members such as MFA, rotating credentials, and restricting access privileges; (b) maintain, test, and monitor the AT&T Defendants' security systems to ensure that Personal Information was adequately secured and protected; (c) timely act upon warnings and alerts to respond to intrusions; and (d) adequately notify the AT&T Plaintiffs and Class Members about the types of data that were compromised in the Data Breach.

753. The AT&T Defendants' duty to use reasonable care arose from several sources, including those set out below.

754. The AT&T Defendants had a common law duty to prevent foreseeable harm to others. The harm was foreseeable because the AT&T Defendants had and continued to sustain a number of data breaches, exposing sensitive information. The AT&T Defendants understand that the exposure of Personal Information can affect individuals' lives for years.

755. This duty existed because the AT&T Defendants collected and stored valuable Personal Information that is routinely targeted by cyber criminals without putting adequate safeguards into place.

756. The AT&T Defendants breached their duties owed to the Plaintiffs and Class Members by failing to maintain adequate data security practices that conformed with industry standards, and were therefore negligent.

757. The AT&T Defendants breached their duties owed to AT&T Plaintiffs and Class Members by failing to exercise reasonable oversight in the selection of Snowflake to store Personal Information. Such reasonable oversight would have revealed that Snowflake's cloud services lacked industry standard data security safeguards necessary to adequately protect Personal Information.

758. The Data Breach was entirely foreseeable. Not only did industry experience show that a failure to adopt the security standards as described herein would result in data breaches, but the AT&T Defendants, themselves, previously experienced a prior breach of a third-party provider by not exercising sufficient oversight over that entity

759. But for the AT&T Defendants negligence, the Personal Information of the AT&T Plaintiffs and Class Members would not have been stolen by cybercriminals in the Data Breach.

760. As a direct and proximate result of the AT&T Defendants' breach of duties, the AT&T Plaintiffs and Class Members have suffered injuries detailed herein.

761. As a direct and proximate result of the AT&T Defendants' negligence, the AT&T Plaintiffs and Class Members are entitled to damages, including compensatory, general, nominal, and/or punitive damages, in an amount to be proven at trial.

SECOND CLAIM FOR RELIEF
Negligence Per Se
On behalf of the AT&T Plaintiffs, the Nationwide AT&T Class, the Nationwide Cricket Wireless Class and the Nationwide Non-Customer AT&T Class

762. The AT&T Plaintiffs repeat and re-allege the allegations contained in Paragraphs 1 through 150, as well Part One and Part Six, as set forth fully herein.

763. The AT&T Defendants had a duty to AT&T Plaintiffs and the Class under the FTC Act as well as statutory provisions concerning the protection of customer information by wireless providers including but not limited to TRPPA and 47 U.S.C. § 222.

764. The FTC Act prohibits "unfair…practices in or affecting commerce," including, as interpreted and enforced by the FTC.

765. Pursuant to the FTC Act (15 U.S.C. § 45), TRPPA, and 47 U.S.C. § 222, Defendants had a duty to provide fair and adequate data security practices to safeguard the AT&T Plaintiffs' and Class members' Personal Information.

766. FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

767. The AT&T Plaintiffs and AT&T Class members were within the class of persons the Federal Trade Commission Act, TRPPA, and 47 U.S.C. § 222 were intended to protect.

768. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act, TRPPA, and 47 U.S.C. § 222 was intended to guard against. The

FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by the AT&T Plaintiffs and AT&T Class members.

769. The AT&T Defendants have admitted that the Personal Information of the AT&T Plaintiffs and AT&T Class Members was wrongfully lost and disclosed to unauthorized third persons, and released on the dark web, as a result of the Data Breach.

770. The AT&T Plaintiffs further believe their Personal Information and that of Class Members was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyberattacks of this type.

771. The AT&T Defendants therefore breached their duty to the AT&T Plaintiff and AT&T Class members by violating Section 5 of the FTC Act, TRPPA, and 47 U.S.C. § 222 by failing to use reasonable measures to protect Personal Information and not complying with applicable industry standards, as described in detail herein.

772. The AT&T Defendants acted with wanton disregard for the security of the AT&T Plaintiffs' and AT&T Class members' Personal Information. The AT&T Defendants knew or reasonably should have known that they had inadequate data

security practices to safeguard such information, and the AT&T Defendants knew or should have known that data thieves were attempting to access databases containing Personal Information such as that entrusted to the AT&T Defendants.

773. The AT&T Plaintiffs' and AT&T Class members' Personal Information would not have been compromised but for the AT&T Defendants wrongful and negligent breach of their duties.

774. But for the AT&T Defendants' wrongful and negligent breaches of the duties owed to AT&T Plaintiffs and AT&T Class Members, AT&T Plaintiffs and AT&T Class members would not have been injured.

775. The AT&T Defendants' failure to take proper security measures to protect the Personal Information of AT&T Plaintiffs and Class Members as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access and copying of Personal Information by unauthorized third parties. Given that companies such as the AT&T Defendants are prime targets for hackers, AT&T Plaintiffs and Class Members are part of a foreseeable, discernible group that was at high risk of having their Personal Information misused or disclosed if not adequately protected by the AT&T Defendants. Because AT&T violated the FTC Act, TRPPA, 47 U.S.C. § 222, and other provisions of the law, it is liable to the AT&T Plaintiffs and Class Members as committing negligence per se.

THIRD CLAIM FOR RELIEF
Invasion of Privacy (Public Disclosure of Private Facts)
On behalf of the AT&T Plaintiffs, the Nationwide AT&T Class, the Nationwide Cricket Wireless Class, and the Nationwide Non-Customer AT&T Class

776. The AT&T Plaintiffs repeat and re-allege the allegations contained in Paragraphs 1 through 150, as well as Part One and Part Six, as set forth fully herein.

777. The AT&T Plaintiffs' Personal Information relating to call and text logs, as well as cell site ID numbers associated with their calls and texts, are of a private, secluded, and highly personal nature, the disclosure of which would be highly offensive to a reasonable person and is not a matter of legitimate public concern.

778. Call and text logs, when combined with cell site identification numbers, can be used to engineer the identity of a customer, as well as their geolocation coordinates, revealing some of the most intimate details of an individual's life.

779. The AT&T Defendants, in failing to implement reasonable cyber security policies and practices, disclosed the AT&T Plaintiffs' and Class Members' Personal Information to cybercriminals and nefarious third-parties, who in turn further disclosed that Personal Information on the dark web by advertising and selling the stolen Personal Information. These disclosures gave publicity to the AT&T Plaintiffs' and Class Members' Personal Information and caused injury.

780. The AT&T Defendants had no legitimate basis to disclose AT&T Plaintiffs' and Class Members' Personal Information to cybercriminals or nefarious third parties.

781. The AT&T Plaintiffs seek all monetary and non-monetary relief allowed by law, including actual, nominal, or general damages; declaratory and injunctive relief, including an injunction barring the AT&T Defendants from disclosing their Personal Information without their consent; and any other relief that is just and proper.

FOURTH CLAIM FOR RELIEF
Violations of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/2, *et seq.* ("ICFA")
On behalf of Plaintiff Hornthal and the Illinois AT&T Subclass

782. Plaintiff Hornthal repeats and re-alleges the allegations contained in Paragraphs 1 through 150, as well as Part One and Part Six, as set forth fully herein.

783. Plaintiff Hornthal brings this claim on behalf of himself and all members of the Illinois AT&T Subclass.

784. Plaintiff Hornthal and Illinois Subclass members transacted for and received telecommunication services from the AT&T Defendants for personal, family, or household services.

785. The AT&T Defendants engaged in unlawful and unfair practices in violation of the ICFA by failing to implement and maintain reasonable security

measures to protect and secure Plaintiff's and Illinois AT&T Subclass members' Personal Information in a manner that complied with applicable laws, regulations, and industry standards.

786. The AT&T Defendants makes explicit promises that they will ensure personal information used on its networks will remain private.

787. Due to the Data Breach, Plaintiff and Illinois Subclass members have lost property and the value of that property in the form of their Personal Information. Further, the AT&T Defendants' failure to adopt reasonable practices in protecting and safeguarding their customer's Personal Information will force Plaintiff and Illinois Subclass members to spend time or money to protect against identity theft. Plaintiff and Illinois AT&T Subclass members are now at a higher risk of identity theft and other crimes.

788. The AT&T Defendants' conduct offends established public policy and is immoral, unethical, oppressive, unscrupulous and substantially injurious to consumers. The harm done sufficiently outweighs any justifications or motives for the AT&T Defendants' practice of collecting and storing Personal Information without appropriate and reasonable safeguards to protect such information in place.

789. As a result of the AT&T Defendants' violations of the ICFA, Plaintiff and Illinois AT&T Subclass members have suffered and will suffer injury, as described above.

790. Plaintiff and Illinois AT&T Subclass members thus seek all monetary and non-monetary relief allowed by law, including injunctive relief, damages, including actual damages in an amount to be proven at trial, treble damages of actual damages, and reasonable attorneys' fees.

FIFTH CLAIM FOR RELIEF
Violations of the District of Columbia Consumer Protection Procedures Act, D.C. Code § 28-3901, *et seq.* ("D.C. CPPA")
On behalf of Plaintiff Lively and the Washington D.C. AT&T Subclass

791. Plaintiff Lively repeats and re-alleges the allegations contained in Paragraphs 1 through 150, as well as Part One and Part Six, as set forth fully herein.

792. Plaintiff Lively and D.C. AT&T Subclass Members are "consumers" under the D.C. CPPA because they received consumer services. D.C. Code § 28-3901(a)(2).

793. The AT&T Defendants are "merchant[s]" under the D.C. CPPA because they "supply the goods or services which are . . . the subject of a trade practice." D.C. Code § 28-3901(a)(3).

794. The AT&T Defendants' telecommunication services and related data collection and storage practices are "trade practices" because they are acts that "directly or indirectly . . . effectuate, a sale, lease or transfer, of consumer goods or services." D.C. Code § 28-3901(a)(6).

795. The AT&T Defendants engaged in deceptive, unfair, and unlawful trade practices prohibited by the D.C. CPPA. D.C. Code §§ 28-3904; 3905(k)(1)

796. The AT&T Defendants engaged in deceptive conduct because, among other reasons, it explicitly and implicitly promises that it will ensure personal information used on its networks will remain private.

797. The AT&T Defendants engaged in unlawful conduct by violating the FTC Act, TRPPA, 47 U.S.C. § 222, and other provisions of federal and D.C. law, including the D.C. Security Breach Protection Amendment Act of 2020 ("D.C. SBPAA"), which provides: "To protect personal information from unauthorized access, use, modification, disclosure, or a reasonably anticipated hazard or threat, a person or entity that owns, licenses, maintains, handles, or otherwise possesses personal information of an individual residing in the District shall implement and maintain reasonable security safeguards, including procedures and practices that are appropriate to the nature of the personal information and the nature and size of the entity or operation." D.C. Code § 28-3852.01.

798. A violation of the D.C. SBPAA, including D.C. Code § 28-3852.01, constitutes a per se unfair or deceptive trade practice under the D.C. CPPA. *See* D.C. Code § 28-3853.

799. The AT&T Defendants violated the D.C. SBPAA, and therefore the D.C. CPPA, by failing to maintain reasonable data security practices to safeguard the Personal Information of Plaintiff Lively and D.C. AT&T Subclass Members, including: (a) failing to implement industry standard data security safeguards to

protect the Personal Information of Plaintiff Lively and D.C. AT&T Subclass Members; and (b) failing to maintain, test, and monitor its security systems to ensure that Personal Information was adequately secured and protected.

800. In addition to its per se violation of the D.C. CPPA, the AT&T Defendants engaged in unfair trade practices prohibited by the D.C. CPPA by failing to maintain reasonable data security practices. D.C. Code § 28-3904.

801. The AT&T Defendants' actions were reckless. As a direct and proximate result of its security failures, Plaintiff Lively and the Subclass Members' Personal Information was subject to unauthorized access and exfiltration, theft, and/or disclosure.

802. The AT&T Defendants' conduct offends established public policy and is immoral, unethical, oppressive, unscrupulous and substantially injurious to consumers. The harm done sufficiently outweighs any justifications or motives for the AT&T Defendants' practice of collecting and storing Personal Information without appropriate and reasonable safeguards to protect such information in place. Consumers could not have reasonably avoided the harm inflicted by AT&T.

803. As a result of the AT&T Defendants' violations of D.C. CPPA, Plaintiff and D.C. AT&T Subclass members have suffered and will suffer injury, as described above.

804. As a direct and proximate result of the AT&T Defendants' deceptive, unlawful, and unfair trade practices, Plaintiff Lively and D.C. AT&T Subclass Members are entitled to injunctive relief, damages, including actual damages in an amount to be proven at trial or statutory damages of $1,500, whichever is greater, treble damages of actual damages, and reasonable attorneys' fees. D.C. Code § 28-3905(k)(1)(A), (k)(2).

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Classes set forth herein, respectfully request the following relief:

A. That the Court certify this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiffs are the proper class representatives; and appoint Plaintiffs' counsel as Class Counsel;

B. That the Court grant permanent injunctive relief to prohibit and prevent Defendants from continuing to engage in the unlawful acts, omissions, and practices described herein;

C. That the Court award Plaintiffs and Class Members compensatory, consequential, general, and/or nominal damages as appropriate, for each count as allowed by law in an amount to be determined at trial;

D. That the Court award punitive or exemplary damages, to the extent permitted by law;

E. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendants as a result of their unlawful acts, omissions, and practices;

F. That Plaintiffs be granted the declaratory and injunctive relief to prevent further injuries from manifesting as alleged herein;

G. That the Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

H. That the Court award pre-and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper; and

I. Any other relief that the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a jury trial in the instant action.

Dated: February 3, 2025

Respectfully submitted,

/s/ Jason S. Rathod
Jason S. Rathod
Migliaccio & Rathod LLP
412 H St NE, Suite 302
Washington DC 20002
Tel. 202.470.3520
jrathod@classlawdc.com

/s/ John Heenan
John Heenan
Heenan & Cook
1631 Zimmerman Trail
Billings, MT 59102
Tel. 406.839.9091
john@lawmontana.com

/s/ Amy Keller
Amy Keller
DiCello Levitt LLP
Ten North Dearborn, Sixth Floor
Chicago, Illinois 60602
Tel. 312.214.7900
akeller@dicellolevitt.com

/s/ J. Devlan Geddes
J. Devlan Geddes
Goetz, Geddes & Gardner P.C.
35 N. Grand Ave.
Bozeman, MT 59715
Tel. 406.587.0618
devlan@goetzlawfirm.com

/s/ Raphael Graybill
Raphael Graybill
Graybill Law Firm, PC
300 4th Street North
Great Falls, MT 59401
Tel. 406.452.8566
raph@graybilllawfirm.com

Co-Lead Counsel for Plaintiffs